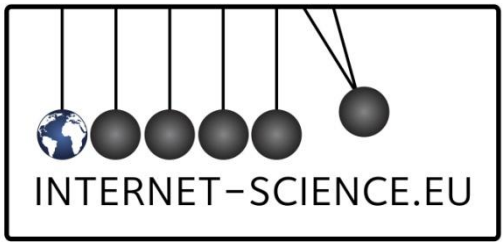
ICT - Information and Communication Technologies



FP7-288021

Network of Excellence in Internet Science

D5.1.1 Overview of Online Privacy, Reputation, Trust, and Identity Mechanisms

Due Date of Deliverable: November 30, 2012

Actual Submission Date: January 30, 2013

Start date of project: December 1st 2011 **Duration:** 42 months

Organization name of lead contractor for this deliverable: OXF

Editors: Samir Passi & Sally Wyatt

Contributors: Samir Passi (KNAW), Sally Wyatt (KNAW), Jo Pierson (IBBT-SMIT), Ralf de Wolf (IBBT-SMIT), Rob Heyman (IBBT-SMIT), Lien Mostmans (IBBT-SMIT), Karmen Guevara (UCAM), Thanasis Papaioannou (EPFL), Alessandro Mantelero (NEXA), Anna Satsiou (CERTH), Iordanis Koutsopoulos (CERTH), Ian Brown (OXF), and Lee Andrews Bygrave (UiO).

Project Information

PROJECT	
Project name:	Network of Excellence in Internet Science
Project acronym:	EINS
Project start date:	01/12/2011
Project duration:	42 months
Contract number:	288021
Project coordinator:	Leandros Tassiulas – CERTH
Instrument:	NoE
Activity:	THEME ICT-2011.1.1: Future Networks
DOCUMENT	
Document title:	Overview of Online Privacy, Reputation, Trust, and Identity Mechanisms
Document type:	Report
Deliverable number:	D5.1.1
Contractual date of delivery:	30/11/2012
Calendar date of delivery:	30/01/2013
Editors:	Samir Passi (KNAW) & Sally Wyatt (KNAW)
Contributors:	Samir Passi (KNAW), Sally Wyatt (KNAW), Jo Pierson (IBBT-SMIT), Ralf de Wolf (IBBT-SMIT), Rob Heyman (IBBT-SMIT), Lien Mostmans (IBBT-SMIT), Karmen Guevara (UCAM), Thanasis Papaioannou (EPFL), Alessandro Mantelero (NEXA), Anna Satsiou (CERTH), Iordanis Koutsopoulos (CERTH), Ian Brown (OXF), and Lee Andrews Bygrave (UiO).
Workpackage number:	WP 5
Workpackage title:	JRA5 Internet Privacy and Identity, Trust and Reputation Mechanisms
Lead partner:	OXF
Dissemination level:	PU (Public)
Version:	Final
Total number of Pages:	103
Document status:	Final
Estimated PM (DOW):	8,5 person months
Estimated PM (spent):	9,25 person months

TABLE OF CONTENTS

Executive Summary

This deliverable provides an overview of the many issues and concerns pertaining to the privacy of users' online personal information, online identity formation, and online trust and reputation mechanisms. The deliverable examines privacy issues as they affect many different Internet applications, but particular attention is given to Online Social Networks (OSNs), one of the most popular and fastest growing technologies. This deliverable provides insights and lessons not only for understanding online privacy, trust, reputation, and identity issues but also for the development of a holistic Internet science view of privacy. The security and privacy of users' personal information online are affected by the following factors:

- technical, including privacy standards and security settings for different devices and platforms;
- social, including how people use online spaces to create and experiment with their identity formation, and who they perceive to be their audience;
- policy regulations regarding privacy, data sharing, and the availability of government data and for research purposes.

Online services are increasingly gaining importance within the everyday lives of people all over the world. Many people, including children and young people, interact with these technologies intensively, and over a prolonged period of time. Moreover, social media and networking platforms allow developers to create particular applications for these platforms. Such large-scale and continuous interactions across online services and applications produce vast quantities of online data that can be combined to produce ever more detailed profiles. These developments have great potential for market research and service innovation, but also raise a host of privacy issues, including: user profiling, third-party data abuse, development and widespread adoption of privacy-invasive social discovery mobile apps, potential privacy threats to minors, and the collapse of a clear distinction between public and private contexts while sharing information online, particularly on mobile devices using location-based features.

This deliverable is divided into three sections: *privacy and design* (technological issues), *privacy and behavior/conduct* (social behavior issues), and *privacy and policy* (policy and regulation issues). Section 2, *privacy and design*, provides an overview of existing privacy, security and encryption methods. Two important conclusions emerge from this section: First, it is difficult for many users to understand the intricacies of data collection, storage, processing, and deletion in the devices and applications they use. These are explicated within the Terms & Conditions and privacy policies of online services, but are often lengthy and ridden with technical and legal jargon. As a means to gather user consent, these are ineffective and thus illegitimate. Moreover, data sharing agreements between online and offline companies raise further privacy concerns owing to the merging of online and offline data into granular user profiles. These agreements are hardly visible to users, as options for opting-out such data collaborations are not even presented on parent sites of online services. Second, the use of specific location-based services in conjunction with data from other OSNs, in the form

of social discovery mobile apps, can lead to privacy-invasive applications of social media, OSN, and mobile data. The combination of personal sensitive mobile information, OSN data, and geolocation tagging on such devices can raise significant user privacy issues and concerns. When users consent to sharing information on two separate online platforms, they do not explicitly consent to these discrete pieces of information being combined. Thus we find that although a number of industry standards and technologies provide users with the means to monitor, regulate, and restrict the flow of their online personal information, much work still needs to be done in order to address and minimize online user privacy issues and concerns. Further investigation into online data gathering, retention, and processing mechanisms as well as into potential uses of location-based data can provide further clarity regarding online user privacy.

Privacy and behavior/conduct are the focus of section 3. Each person interacts with and uses online services and applications differently. Some users use online social media and networking services in order to develop and maintain a particular online identity, others use them simply as tools for communicating with colleagues, friends and family online. Users vary in the extent to which they are aware both of privacy-threatening uses of social media and the means available to them to prevent privacy breaches. This also raises challenges for the industry, as can be seen in its inability to accurately translate social, behavioral and privacy norms and conduct into technological options and features. Section 3 also pays attention to the specific needs and problems faced by children and young people when using social media and networking services. The widespread belief that young users do not care about their own online privacy is incorrect. Research has shown that young users are as concerned about their online privacy as adult users are. Nonetheless, young users often find it difficult to comprehend the online privacy policies and regulations (sometimes ignoring such policies altogether), making them vulnerable to online privacy breaches.

Section 4, *privacy and policy*, examines the ways in which governments are responding to the challenges raised by the creation and sharing of data online. Government agencies have to audit and regulate industry standards, mechanisms, and technological tools that are used for collecting, storing, and processing online user information. Policy makers face many technological and managerial challenges, ranging from the difficulty of incorporating privacy by design across web services and applications to managing independent/unregulated technology development processes. Countries and regions deal with user privacy issues and concerns differently. EU member states follow a detailed and comprehensive data use and privacy policy, largely shaped by the 1995 EU Directive on the protection and movement of user data, whereas the USA has a much more fragmented approach towards user privacy. However, data on the Internet is not bound by political boundaries, making its regulation even more difficult. Furthermore, some sharing of data is legitimate for law enforcement and commerce. Balancing these legitimate needs with those of individual privacy remains a technical and policy challenge.

Section 5 summarizes the main conclusions and provides the following suggestions for future research about privacy in relation to *design*, *behavior/conduct*, and *policy*.

Privacy and Design

- What are the current technological means of collecting, storing, processing, and deleting users' online personal information? How can these be classified?
- How are cookies used across online services? What is the nature of users' personal information and online activity tracked and transmitted by cookies?
- What are the privacy implications of social and behavioral advertising on online social media and networking technologies?
- What are the existing data collaboration agreements between online services? What is the nature and content of data shared across services?
- How can privacy policies be presented to the user in more conspicuous and easily-readable forms without undermining their technological and legal essence?
- What steps need to be taken to increase the uptake of PPETs such as DSNs in comparison with mainstream applications and services?
- What are the potential privacy-invasive combinations of location-based services and social media and networking information? How can user privacy and security concerns be addressed?
- What are potential uses and abuses of Big Data?

Privacy and Behavior/Conduct

- What are the uses of online social media and networking services? What different related privacy issues and concerns do they raise?
- How do users perceive intended/unintended and visible/invisible audiences?
- How can we minimize the privacy paradox in terms of finding a balance between necessary privacy settings and effective management of data by users?
- What is the feasibility and effectiveness of the privacy by contextual integrity approach?
- How do minors and young adults use social media and networking services particularly on mobile devices?
- What means and mechanisms can be developed to enable the use of publicly available data for research purposes in ways that preserve the privacy of user information?

Privacy and Policy

- How can 'privacy by design' be incorporated within the lifecycle of already developed and deployed services such as Facebook and Google+?
- In the wake of rapidly evolving nature of web applications, how can privacy-invasive events be predicted and modeled?
- What are the minimal data collection limits across web services and applications?
- What steps need to be taken to bridge the gap between policy making processes and their subsequent technological and managerial implementation? For example, what steps need to be taken to implement Article 17 on online social media and networking services?
- How can existing data use/privacy policies be made globally interoperable?
- What steps need to be taken to ensure the regulation and management of user privacy within independent/unregulated technology development processes?
- What are the differences between traditional online services and mobile devices and apps? What further steps are needed to ensure the development and enforcing of effective data use and privacy policies across mobile devices and applications?

List of Figures, Tables, and Boxes

1. Introduction: Information Privacy in the age of Online Social Networks

This deliverable explores the multiplicity of issues and concerns pertaining to the privacy of users' online personal information, online identity formations, and online trust and reputation mechanisms. Online Social Networks (OSNs) have become an integral part of contemporary technological cultures, and thus provide a good example for exploring these issues. In recent years, social networks such as Facebook, MySpace, Twitter, and Google+ have gathered large numbers of users. Facebook, one of the most popular OSNs, recently announced that its monthly active user base has surpassed the one billion mark (Facebook, 2012), and with this the number of users on Facebook now exceeds the population of all the countries in the world with the exception of India and China.

Users are of all ages and nationalities. Part of the broader category of Online Social Media applications, which can be seen as a form of mass self-communication (Castells, 2009), OSNs represent virtual communities in which people interact with each other and in turn produce vast amounts of information through these interactions. The nature of these user interactions varies from one OSN to another and takes many forms such as profile pictures, status messages, wall posts, private messages, tweets, photographs, comments, location data, likes, ratings, and more. This deliverable focuses on the multiplicity of issues concerning privacy, reputation, trust, and identity in relation to the information generated by such user interaction on OSNs. Such an analysis provides widely acceptable insights and lessons not only for understanding online privacy, trust, reputation, and identity issues but also for the development of a holistic Internet science view of privacy.

All major OSNs enable and facilitate large-scale user interactions within virtual communities, and also provide certain tools to software developers, allowing them to build application and services that can be integrated within social networks. Examples of such applications include the Nike mobile app[1] , allowing users to share details of their daily runs on social networks such as Facebook. Examples of services include the ability to use one's Facebook login credentials to log into other social media websites. Furthermore, with the widespread diffusion of mobile devices such as smartphones and tablets, a large number of mobile apps have been developed that enable and facilitate user interactions with OSNs and related third-party applications and services. Such applications and services have implications for a user's online privacy and these issues will be explored in detail further in this report.

Another important aspect in relation to the use of OSNs is the widespread diffusion of mobile devices such as smartphones and tablets. A large number of mobile apps exist that allow users to access, interact, and search within a number of OSNs simultaneously. While some of these applications are developed by the online social networking organizations themselves (e.g., the Facebook mobile app), a far greater number of third-party applications have now come up that not only allow a user to access and interact with a number of OSNs but also provide novel means to either search for other people online or aggregate information

[1] See: http://nikeplus.nike.com/plus/products/gps_app/

in non-traditional ways (e.g., TweetDeck or other Social Discovery Platforms[2]). The growing use of mobile devices is evident in the fact that Facebook has recently announced that as of September 2012 there are 604 million monthly active users who use its mobile products (Facebook, 2012).

An important privacy concern in relation to the use of mobile devices to access OSNs is the user's location data and mobile identifiers that are involved in such interactions. Mobile apps have access to a user's personal information on the mobile device (such as contacts, location, photos, messages etc.) in addition to the user's OSN. Such coupling facilitates information convergence and this sometimes leads to situations where a user's privacy is compromised. For example, over the years certain mobile apps have been developed that allow a user to explore his/her vicinity to search for young girls plus women around his/her location.[3] Thus, the use of mobile devices to interact with OSNs' data and services has implications for privacy, reputation, trust, and identity issues online and this deliverable also focusses on these issues in relation to the growing use of mobile devices. Before moving further with the report, section 1.1 provides a brief history of online social networks along with a few of their prominent characteristics, and section 1.2 explains the structure of this deliverable.

1.1 | Overview: The turn towards OSNs

One of the earliest variants of OSNs was Usenet, a bulletin board service that connected Duke University and the University of North Carolina (Curtis, 2011). Developed by two Duke University graduate students in 1979, Usenet allowed for online discussions where users could read and post content within particular groups. Since then, as the Internet became publicly available in 1993, a large number of other OSNs catering to forums, blogs, and multimedia content were developed. Early examples of these include SixDegrees.com, AOL messenger, and Friends Reunited.

However, it was at the dawn of the 21st century that social media sites gained prominence on the Internet. In 2002 Friendster was launched and it soon grew to three million users in just under three months (Ibid.). Following the success of Friendster, MySpace, along with LinkedIn, was launched in the year 2003. The year 2004 marked an important milestone with the development of Facebook, an OSN developed by students at Harvard University. Although Facebook was initially restricted to college and high-school students, in 2006 anyone over the age of 13 was allowed to become a Facebook member. This was the same year that Twitter, the microblogging service, was launched.

Moreover, in 2007 Facebook initiated a service called Facebook Platform that allowed third-party application developers to build applications and services for the social network. Post-Facebook, a large number of OSNs catering to different kinds of audience have come up on the World Wide Web (WWW). Examples include Orkut, Google+, Foursquare, Hi5, and

[2] See subsection 2.3.a of this report for an explanation of Social Discovery Platforms.

[3] See, for example, the mobile app called 'Girls Around Me'

Hvyes, and Netlog. However, although a large number of OSNs exist on the Internet, Facebook has regained prominence amongst them and its user base has grown rapidly from 200 million users in 2009 to one billion users in 2012, a growth rate of approximately 400% in just over three years.

This growing use of OSNs has facilitated the Internet phenomenon of 'Sharing' – which is one of the key characteristics of such networks. Since OSNs are user-generated content systems, the working of these systems depends on the assumption that users will share and distribute information online. This has led to the current situation in which social sharing buttons and services are present on almost every website. With the click of a button, links, content, pictures, and virtually everything else can be instantly shared with one's OSNs. With over a billion people online, such a large-scale information sharing and distribution network creates vast amounts of data every day. Moreover, third-party applications and services allow for integration of data across online networks and this has further implications for the large-scale convergence of information enabled and facilitated by OSNs. Figure 1 provides an infographic further depicting the history of social media and social networking sites.

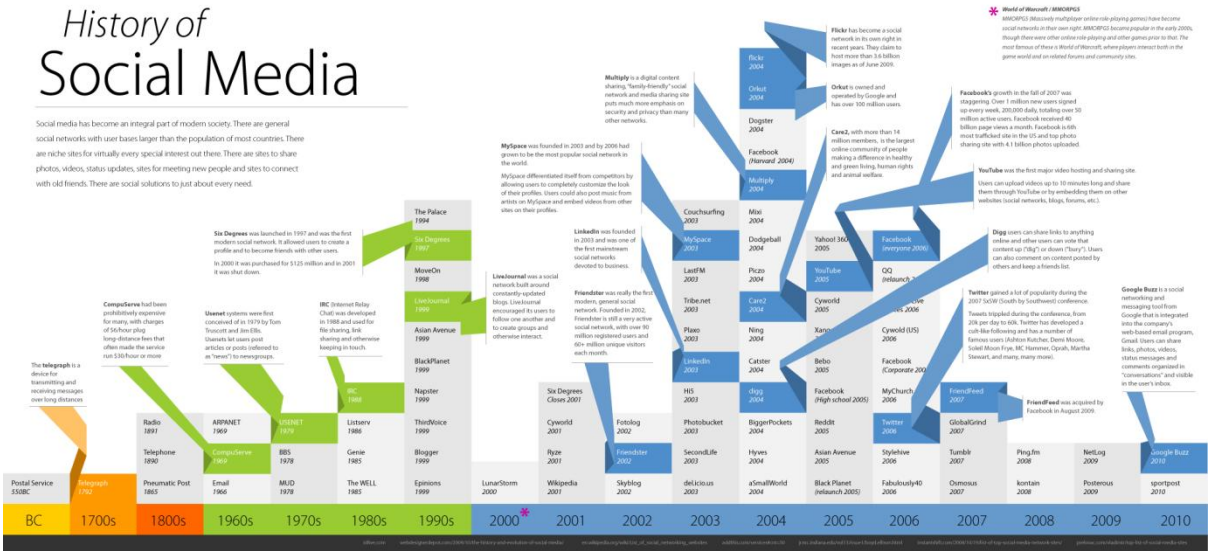


Figure 1: A Brief History of Social Media[4]

Concerning the issues of privacy, trust, reputation, and identity in relation to OSNs, there are a few prominent characteristics of information on OSNs that deserve special attention:

- **Tagging**
  - Tagging is the process by which the user, or automatic scripts, assigns different kinds of identifying information to a particular piece of online content. For example, when user A posts something on user B's profile, the OSN scripts tag the content as 'communication from A to B'. This makes it easier to see all

[4] Source: http://www.ritholtz.com/blog/wp-content/uploads/2010/12/socialMediaTL_05.png

communication between A and B with the help of just one button. Moreover, a user might also explicitly tag the information to contribute to a particular discussion online or showcase where and when a particular picture was taken.

- **Instantaneous Nature**
  - The instantaneous nature of OSNs refers to the fact that these networks operate in real-time. Content posted on one of the OSNs instantly reaches a wide audience. This has implications for the situation when a user realizes that he/she may wish to delete particular bits of information later owing to the highly persistent nature of online information (boyd, 2008). Since the information is already transmitted to a large audience, who can download and archive that information during that time, it makes it very difficult to remove already existing online content. Coupled with the self-replicating nature of online information this makes it even more difficult to prevent the spread of a particular piece of information. Sharing is a key process online, and often particular content posted by one user soon becomes viral and reaches a large number of people both within and across the original user's online social groups.

- **Outreach**
  - A key characteristic of information on OSNs, in contrast to offline information, is its large-scale outreach. In addition to the facilitation of information generation, the broadcasting nature of the Internet, and particularly that of OSNs, fosters online spectatorship, marking an increased exposure and access to information (Balkin, 2004). Content posted on a social network is accessible to a wide audience ranging from one's friends and friends of friends, and sometimes even publicly available to every other user on network.

- **Searchability**
  - One of the most important attributes of users' personal information on OSNs is its searchability. A popular belief concerning online search is that it is very difficult to search for and find specific information online. Indeed researchers have pointed out the difficulty of using search engines to find relevant information online (Morris, Teevan & Panovich, 2010; Wouters, Hellsten & Leydesdorff, 2004). However, OSNs are quite different from search-engines and their granular structure often makes finding particular people and related information a lot easier.[5] For example, most online user profiles are linked to

[5] This is clearly evident within Facebook's Graph Search – a recently launched feature that allows users (and online advertisers to search through their friends and user base to search for people with particular interests, activities, and other personal information. For example with Graph Search one simply has to ask questions such as 'how many of my friends are single?' to receive instant results.

particular email addresses, which make it quite easy to search for particular users. Moreover, even if the email address is unknown the ability to refine OSN search results by place of birth, academic institution, work place etc. makes it easy to find particular people on specific social networks.

- **Social Convergence**
  - Social Convergence refers to the process of large-scale convergence of information across OSNs and mobile devices. Using third-party applications and services, it is now possible to simultaneously search for and access information from not one but multiple OSNs. Moreover, mobile devices often tag user content with a user's location and mobile identifier data. This enables data convergence not only within and across OSNs but also between virtual interactions and physical user location. Furthermore, most users use the same email address, a unique identifier on OSNs, across multiple social networks and this can be used to enable user profiling across networks.

1.2 | Report structure: Design, Behavior/Conduct, and Policy

This deliverable presents a detailed overview of the relationships between OSNs, users, and the issues of trust, privacy, identity, and reputation. These issues are not only technological in nature. Ways of ensuring information security and privacy represent only one particular dimension of the societal concerns around the privacy of a user's online information. These issues are embedded within the larger narrative comprising the ways in which people interact with and use OSNs, the social norms and practices concerning user privacy, and government and industry privacy regulations and policies. Within this context, the privacy, reputation, and trust issues concerning the use of OSNs can be interpreted within the three interrelated domains of technology, social behavior, and policy and regulation.

Technological issues include, for example, the ongoing practices and methods of data collection and user profiling on OSNs. Social behavior issues include the ways in which users interact with OSNs and the difficulties that they encounter in trying to secure their online content. Finally, policy and regulation issues include the challenges and difficulties faced by governmental, as well as industrial, organizations in relation to the security and privacy of users' personal information online. To address the multiplicity of issues concerning the privacy of users' OSN information, this deliverable has been divided into three sections: *privacy and design* (technological issues), *privacy and behavior/conduct* (social behavior issues), and *privacy and policy* (policy and regulation issues).

2. Privacy and Design

This section deals with the technological issues concerning online information and data privacy. It focuses on practices of data collection, user profiling, and targeted advertising used by private industry (section 2.1) and also on the ways in which privacy-preserving technologies such as distributed OSNs manage user privacy concerns (section 2.2). A special focus in this section is on issues of privacy in relation to the use of mobile devices, such as smartphones and tablets, to access and interact with data on social media services and OSNs. Mobile devices contain a large volume of users' private information such as contacts, photos, and messages. Moreover, with the advent of location-based services a vast majority of mobile device applications nowadays use users' location data to provide personalized and contextual services. In this regard, section 2.3 deals with issues of privacy in relation to the use of OSNs and social media services on mobile devices.

2.1 | Personalized web experience and issues of Privacy and Trust

The term 'social' in 'social media and networking' refers to the particular characteristic of such technologies to enable and facilitate large-scale communication and correlation amongst online users. Users of social media sites and OSNs use these online networks to generate, share, link, and transmit information amongst each other. In turn, OSNs store and process user-generated content to provide users with personalized profiles and social environments. For example, in Facebook every user sees a unique consolidated collection of his/her friend's recent posts, activities, likes, and other information in the 'news feed' page based on his/her profile settings, social interaction history, and installed OSN applications. This is also the case across most social media and networking services online including, but not limited to, Google+, MySpace, Foursquare, Spotify, Hvyes, and Pinterest.

Moreover, in addition to OSNs, various third-party OSN applications and trackers also store and process user information on these networks. Although some of these applications and trackers need to be explicitly installed by users, a few trackers are embedded within the page code and remain invisible to the users, such as the Google Analytics tracker. The information collected by these applications and trackers is then used either to provide specific recommendations to users (such as that for music bands and movies) based on the activity of their friends or to display contextual user-specific advertisements (such as that for clothing and perfumes) on OSNs and other affiliated websites based on related user and friend activity. In this regard, figure 2 explains how third-party cookies are used for advertisement tracking on websites.

However, to provide such a personalized online social experience to users, OSNs and third-party companies gather, store, process, and correlate large amounts of users' personal information. Although the collection of certain information (such as name, email address, and IP address) is sometimes essential to authenticate users, to prevent online fraud, or to ensure the proper functioning of web services, the collection and processing of user data at a granular level often raise a host of privacy issues and concerns. For example, OSNs often consolidate user information across web services to create a detailed profile of a user's personal

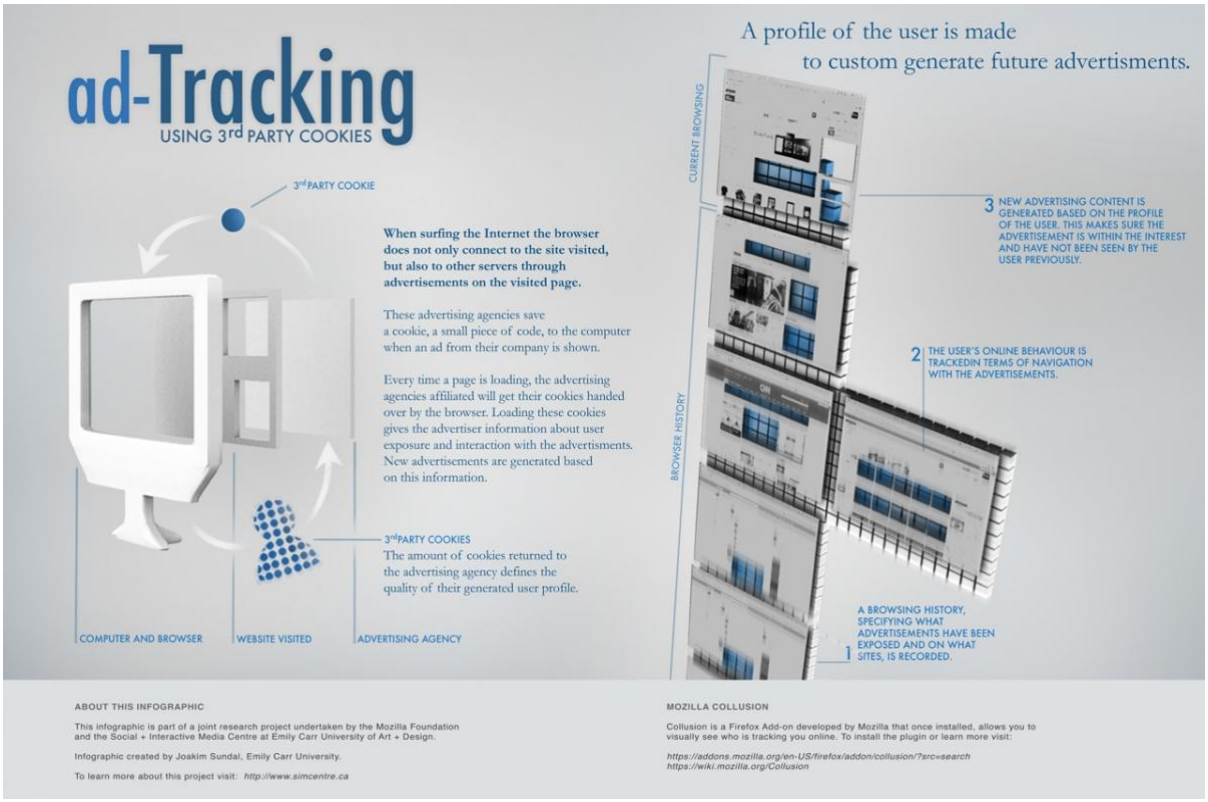


Figure 2: How ad-Tracking works [6]

information and online activity.[7] This profile may also include information on a user's geographical locations as well as his/her ecommerce transaction history. This profile is then used by first- and third-party companies to target users with intrusive contextual advertisements (Cho, 2004) . Box 1 provides further examples of privacy issues and concerns raised due to currently existing industry practices of data collection and user tracking.

Such issues and concerns mostly stem from existing industry practices and technological means employed by online social media and networking services. Using sophisticated technological means, online companies gather and process users' personal information and online activity to provide further personalized and contextual services to their users. Moreover, the privacy policies of these websites are quite lengthy and difficult to understand and users often not only find it difficult to understand the privacy settings on these websites but also feel that the existing privacy features fail to address their concerns (see, for example De Wolf (2013), FTC (2012), and Madden (2012)). Nonetheless, users often proactive take charge of their online privacy by using techniques such as social steganography[8] (boyd and Marwick, 2011). Broadly, in relation to the industry practices and technological means

[6] Source: http://www.simcentre.ca/sites/simcentre.ca/files/uploads/poster_sundal_large_web_1280x831.jpg

[7] For example, refer to Facebook's data use policy pertaining to Facebook's Social Platform technology (https://www.facebook.com/about/privacy/your-info-on-other)

[8] Social steganography refers to the process of contextualizing a piece of information in such a way that only a particular target audience can understand the real underlying message.

employed by social media services and OSNs, a vast majority of issues concerning the security and privacy of users' online personal information stem from five categories:

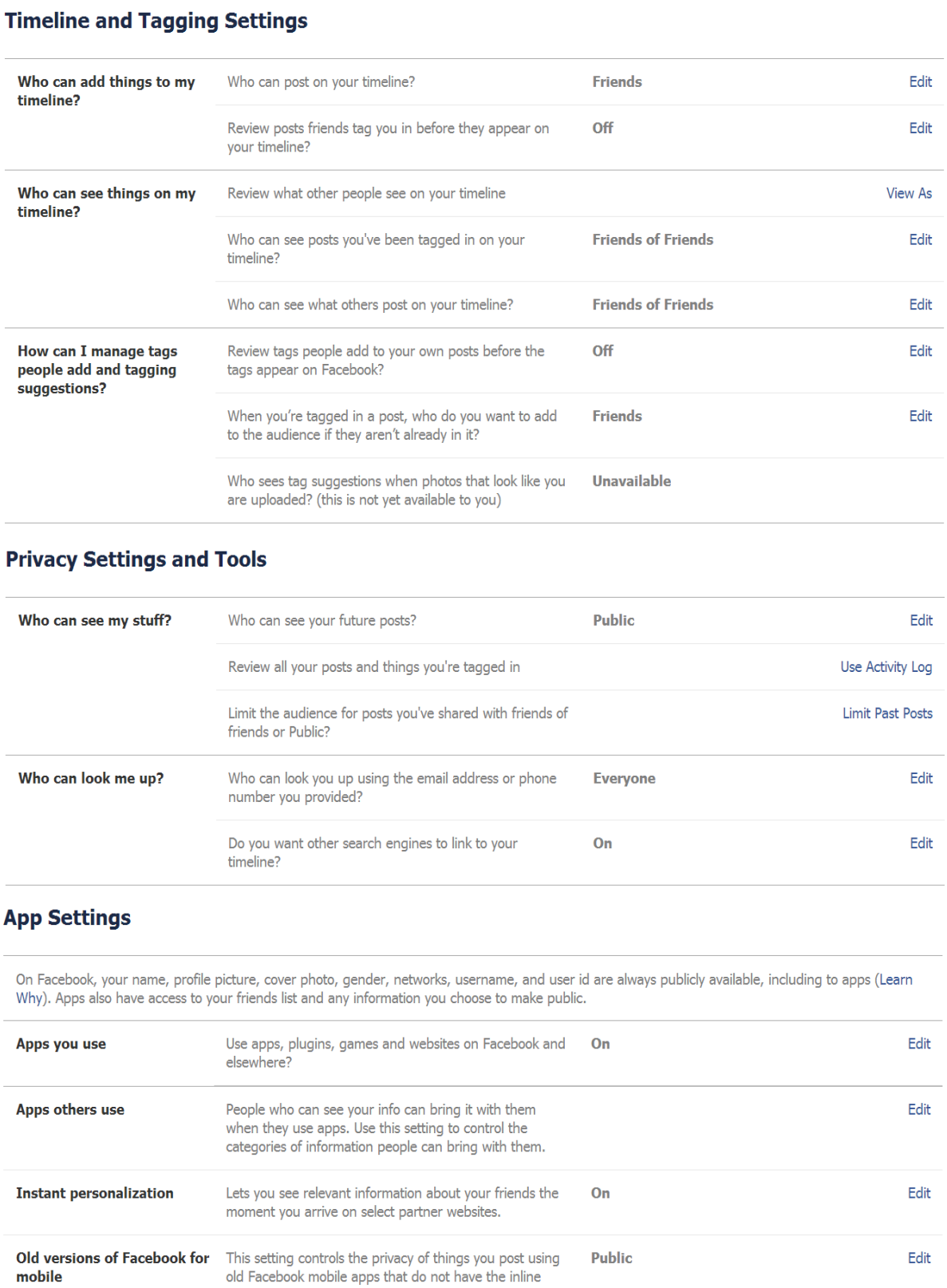
- Default sharing permissions on OSNs provide bare minimum privacy;
- Online services track user activity and information for commercial purposes;
- Users profiles are created to target them with personalized advertisements; and
- Social media services and OSNs often have very little or no liability concerning the privacy of users' personal information.

Box 1
Privacy issues and concerns raised by existing online industrial practices

- Stalking of particular users whose personal information is available online
- First-parties disclosing user information to third-parties and other business organizations
- Highly intrusive and non-user friendly social media and OSN privacy policies which usually indicate that shared user information not only belongs to the social network organization but will also be used for commercial purposes and market research
- Use of online services by minors and young adults who often do not fully understand the often complex privacy and data use policies and mechanisms on such services

a) Public by default – private by effort

Since social media services and OSNs thrive on user-generated content and communication, it is in their commercial interest to enable and facilitate as much user data generation and sharing as possible. Moreover, in today's era of social media connectivity and interoperability of information between these services, most social networks (as also explained earlier in the Introduction) provide means for developers to create custom applications and services that can be installed on the social platform itself. Nonetheless, OSNs and social media services provide users with particular privacy settings to manage and regulate the nature and content of the information that they share within and across platforms and services. However, when a user creates a new profile the default privacy settings are usually set at a level that provides minimal levels of privacy to users. Figure 3 shows the default privacy settings of a newly created profile on Facebook. As can be seen, most of the default settings for timeline, tagging, and applications is set quite openly. Moreover, all the 'review before posting' options are also disabled by default while the option to index the profile within search engines is enabled.



Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	**Friends**	Edit
	Review posts friends tag you in before they appear on your timeline?	**Off**	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	**Friends of Friends**	Edit
	Who can see what others post on your timeline?	**Friends of Friends**	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	**Off**	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	**Friends**	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	**Unavailable**	

Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	**Public**	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can look me up?	Who can look you up using the email address or phone number you provided?	**Everyone**	Edit
	Do you want other search engines to link to your timeline?	**On**	Edit

App Settings

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps (Learn Why). Apps also have access to your friends list and any information you choose to make public.

Apps you use	Use apps, plugins, games and websites on Facebook and elsewhere?	**On**	Edit
Apps others use	People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.		Edit
Instant personalization	Lets you see relevant information about your friends the moment you arrive on select partner websites.	**On**	Edit
Old versions of Facebook for mobile	This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline	**Public**	Edit

Figure 3: Default privacy settings on Facebook [9]

[9] The screenshot is taken from a recently created user profile (January 5, 2013) that was made specifically for the purpose of this research.

Although users can later change these settings, the fact that by default OSNs and social media services want users to share as much information as possible depicts how within online social environments information is public by default and private only by effort on the user's part. Nonetheless, OSNs such as Facebook often put a lot of effort into explaining the privacy settings to the users.[10] However, these organizations constantly change their privacy policies without consulting with their users, making it difficult for users to understand the policy changes.

The fact that the default settings on OSNs are set at minimum levels might lead people to assume that perhaps users prefer sharing more information publicly. However, this is definitely not the case. In fact, when asked, a vast majority of users indicate that they have had to change their privacy settings at some point in time because they felt they were either sharing too much information online or they felt that some or all of the information they share is for a particular audience and not for everyone (Madden, 2012). In a survey conducted by the Pew Research Center in the USA, nearly 80% of the respondents indicated that they have changed their privacy settings to a more restrictive level while 63% of the users indicated that they have 'unfriended' certain people as well. Furthermore, nearly 50% of the respondents indicated that they experience some levels of difficulty while managing and regulating privacy controls on these sites (Ibid.). Figure 4, taken from the Pew report, illustrates the privacy settings of online users by age groups.

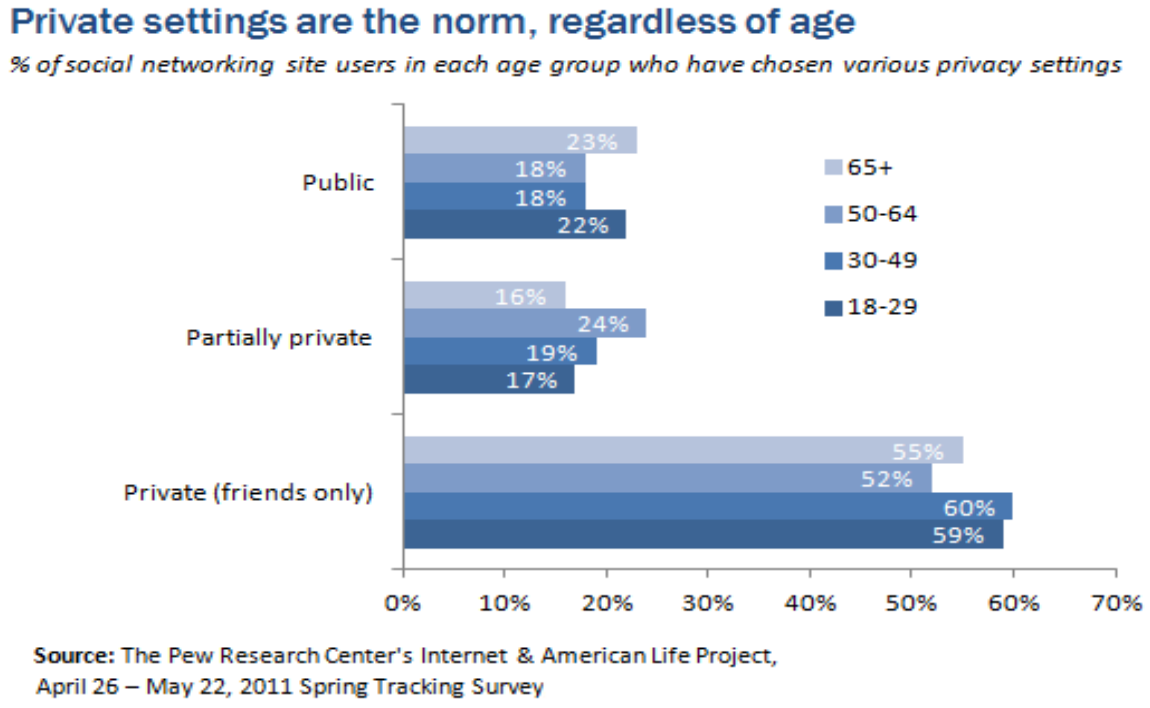


Figure 4: People are increasingly making their profiles private

[10] Facebook recently launched a new feature called 'Privacy Shortcuts' which allow users to easily access and modify their privacy settings.

b) Data tracking

OSNs and social media services track user data in a variety of forms primarily through the use of specific kinds of cookies. A web cookie can be understood as a file that is stored on a user's computer by online services while he/she interacts with these services. This cookie then remains on the user's computer and when the user visits or interacts with the site again, online services can retrieve these stored cookies to examine the user's web history as well as his/her previous interaction with the service. Figure 5 provides a visual description of the relationships between third-party cookies, data tracking, and website use.

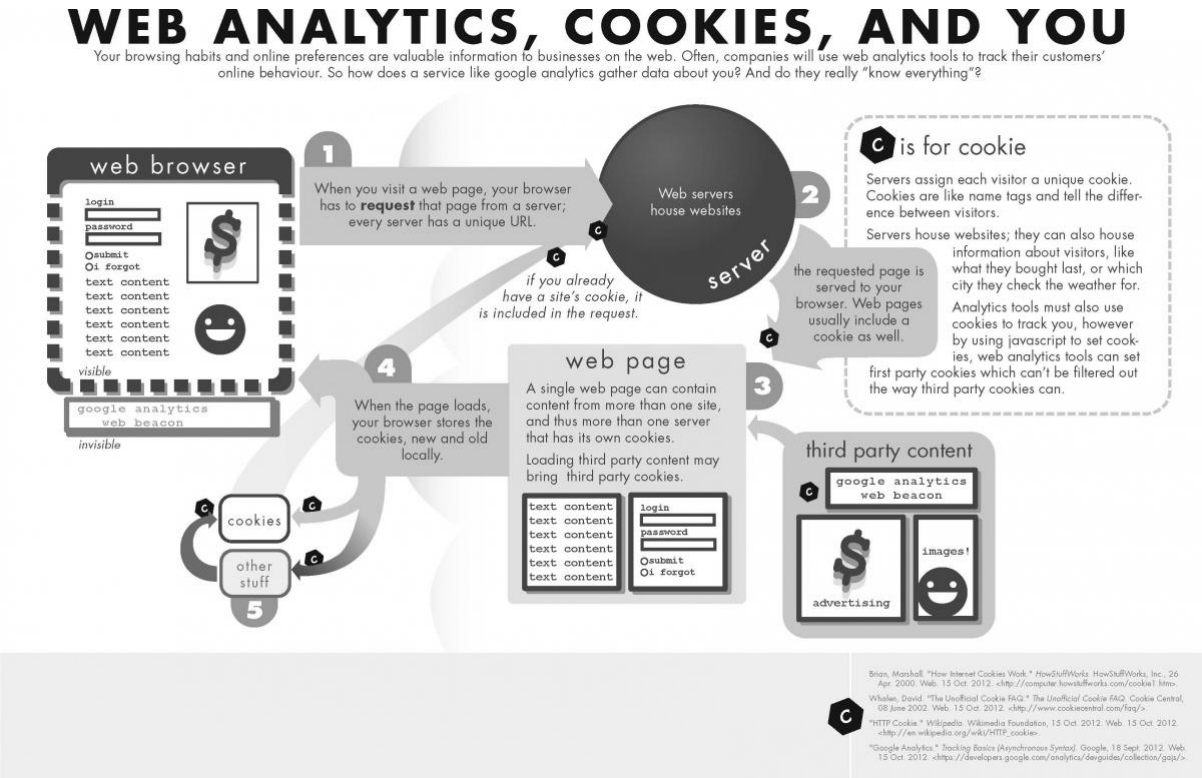


Figure 5: Mozilla Collusion Project Infographic on Web Analytics and Cookies [11]

The three most important types of cookies are:

- **Session cookies**
  - A session cookie is created by online services to mark a user's currently active login session on the website. These cookies are usually deleted by the web browsers when the users log off from these services. Such types of cookies are only stored within the temporary memory space and not on the hard disk itself.
- **Persistent cookies**
  - A persistent cookie has a much longer shelf-life in comparison to the session cookie. Moreover, this kind of cookie is not deleted after the user logs off the service and is usually stored on the user's hard disk. Whenever a user returns

[11] Source: http://www.simcentre.ca/blog/admin/mozilla-collusion-project-infographic-web-analytics-cookies-you

to the web service that installed this cookie, the service can read/write data to the cookie.

- **Zombie cookies**
  - Zombie cookies are special cookies that are automatically recreated once the user deletes them from his/her device. This is done either using specific scripts for cookie-generation or through the cookie backups stored within the user's device at non-traditional locations.

In addition to the tracking of user data by first-party websites, there are also a large number of third-party services and applications that gather, store, and process users' personal information and online activity for commercial purposes such as for targeted advertising, for gathering analytics about a particular online service or web page, and for gathering user activity data for market research or bug reporting. There are certain industry standards that allow users to limit or block these trackers from gathering and storing information about their online activities[12], however, these trackers are usually invisible on a particular web page or online service which could mean that users are often not even aware that they are being monitored. Table 1 provides the names of few primary third-party trackers sorted according to utility:

Online Advertising Trackers used primarily for targeted advertising purposes				
24/7 Media	33Across	Accelerator Media	AccessTrade	actionpay
Web Analytics Trackers used primarily for collecting web analytics				
Alexa	Adara Media	Google Analytics	AdPlan	3DStats
Beacons Invisible scripts to examine whether a user has interacted with specific elements of a site				
AdBull	AdInsight	AdInsight Clarity	2leep	Acerno
Widgets Small executable codes installed on sites and executed when a user interacts with the service				
ActiveConversion	AdKeeper	Adobe Tag Container	apptap	Apture

Table 1: Third-party trackers and user tracking

[12] This includes, for example, the Do-Not-Track initiative. This is explained further in section 2.2.a.

c) Social and behavioral advertising

The data collected by first- and third-party services, trackers, and widgets is often used to create a detailed user profile containing data aggregated across time and web services. A primary use of such user profiling is in targeted advertising. This entails the use of already collected user information and web activity to target specific advertisements to the user. The nature and content of the advertising depends not only on the platform on which the advertisement is displayed but also on the nature of the data that is used to target the advertising.

For example, there is a difference between an advertisement for a product that the user him-/herself likes and an advertisement for a product that is recommended to the user because his/her friends like the product. This practice of targeted advertising is further facilitated by the fact that nowadays a user can use his/her social networking profile, such as that of Facebook, to log in and use a host of other services such as news media sites, music services, video services, bookmarking sites, and content curation services. This enables these social networking sites not only to collect data on the nature of sites that a user frequents but also to track user activity across online services.

In this regard, figure 6 provides an infographic which uses the particular example of Facebook 'likes' to illustrate how user activity is tracked and profiled across websites. Furthermore, figure 7 depicts an infographic containing information on how certain websites gather user information, the nature of content that these websites gather, and what this stored information is then used for. In addition to this information, the infographic also provides data on the approximate revenue that Pinterest, Google, Facebook, Twitter, LinkedIn, and Pandora earn due to online advertising.

Online targeted advertising is of various kinds, including:

- **Search engine advertisements**

  These advertisements are based around a user's browsing and search history. Search engines install persistent cookies on user devices, allowing them to track a user's search history across online as well as offline sessions in which the user interacts with the search service.

- **Social networking advertisements**

  Social networking advertisements are primarily based on a user's social media and networking information. These advertisements are quite personalized and change from time to time depending upon related user and friend activity on social networks. For example, if you like the page of a particular product (such as that of Calvin Klein) on Facebook, an advertisement might appear in your friend's news feed informing him that you like this specific product. Facebook has also been known to target advertisements based on a user's personal information such as relationship status. A user who is 'engaged' might see advertisements for products such as wedding dresses.

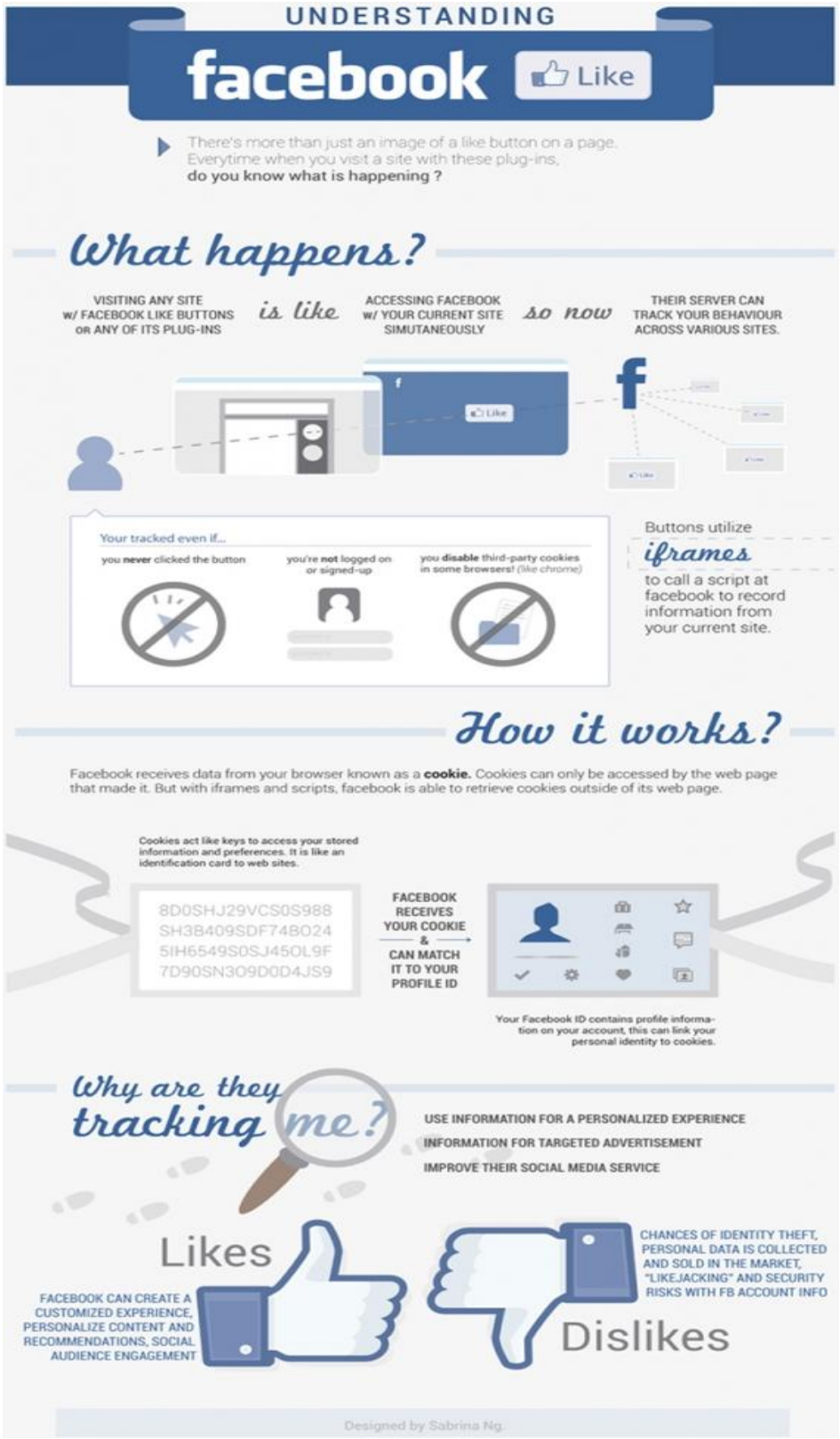


Figure 6: How Facebook 'Likes' work [13]

[13] Source: http://www.simcentre.ca/sites/simcentre.ca/files/images/poster_ng_large_web_709x1497.jpg

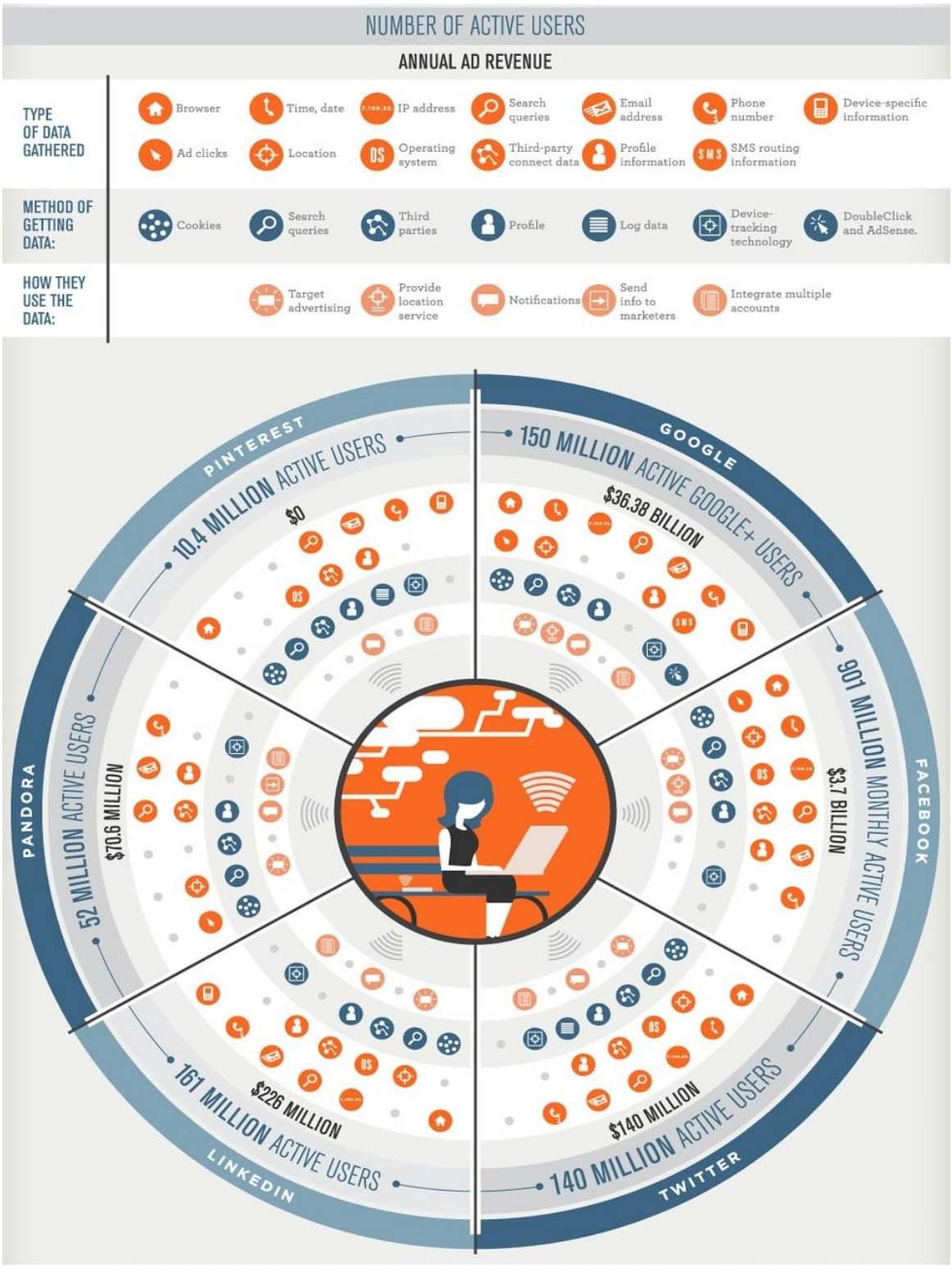


Figure 7: Advertisement marketing on OSNs [14]

[14] Source: Infographic created by company called Baynote (http://www.baynote.com/infographic/i-know-what-you-did-on-the-web/)

- **Behavioral advertisements**

  Behavioral advertisements are primarily based on a user's online browsing as well as ecommerce history. Industry agreements allow online services to share information amongst each other, allowing particular online services to target users with specific advertisements. For example, if you like 'perfumes' on Facebook and/or have brought a perfume from an online shopping website – you might encounter advertisements for perfumes on unrelated websites such as news media websites and social bookmarking services.

d) Social network organizations and user data

Users on online social media and networking services are often greatly concerned about 'who' is able to see the information that they share (see Debatin, Lovejoy, Horn & Hughes, 2009) instead of how the online service itself processes and uses their information (Hashemi, 2009; Raynes-Goldie, 2010). Research has shown that the technological affordances of OSNs pertaining to user privacy are primarily aimed towards social privacy (*which users and applications can access the information*) while the users have little or no control over informational privacy (*the nature of user information and activity collected by OSNs and advertisers*) (De Wolf, Heyman & Pierson, 2012). Security and privacy lapses by social media and networking industries themselves are often revealed only in the form of particular cases and incidents. A recent example of this is the controversy over Facebook's facial-recognition tool in Europe. After Facebook launched its facial-recognition technology to identify particular users within uploaded photographs for purposes such as suggesting face tags on newly uploaded pictures, the tool soon fell under the scrutiny of the Irish Data Protection Commissioner (Bradshaw, 2012). In a recent audit the commissioner formally asked Facebook to disable its 'tag suggest' feature and to delete the facial-recognition database. Although Facebook believes that its facial data collection mechanisms comply with EU laws, countries such as Germany and Norway do not seem to agree to such claims. Recently, Facebook has agreed to shut down this feature across Europe. However, the exact details of how this will be implemented and what will this imply for users with friends in different continents still needs to be ascertained.

Moreover, privacy issues are also raised when social media organizations share and process information amongst each other. One such incident was the Facebook beacon case. Beacon was a Facebook program that collected and transmitted information from third-party websites back to Facebook. The aim of the program was to provide targeted advertising to users based on their activity on other web services and applications. There were two main problems with the initial variant of the program which led to privacy concerns: a) Beacon shared and published user information on Facebook without gaining the user's explicit consent, and b) it also collected and published information related to people who had either deactivated their Facebook accounts or had never signed up for Facebook (Havenstein, 2007). Facebook later deactivated the Beacon service in 2009.

These are two isolated examples but they indicate the extent to which social media organizations collect and store data on each user as well as how data migration across social platforms can lead to severe privacy issues and concerns. Recently Facebook has made a significant addition to its advertising services by partnering with Datalogix – a data analytics firm that monitors shopping transactions of over 70 million Americans across 1000 retailers (Bea, 2012). Datalogix can correlate its data with Facebook profiles by matching the email addresses of users. This provides Facebook with a unique capability to further enrich a Facebook user's online profile with his/her offline shopping transactions, thereby raising privacy concerns over the extent to which users would like such granular consolidation of their online and offline data. Furthermore, there is no opt-out feature available for this on Facebook's website itself and users currently have to visit Datalogix's website to opt-out of this tracking.

The existence of such partnerships shows how social media and networking organizations are increasingly collecting, storing, and processing large amounts of users' personal information not only across online services and applications but also across offline transactions and user activity. This not only calls for a detailed review and audit of existing data migration mechanisms between mainstream social media and networking services but also necessitates that users should be further notified and educated about how online services are using their personal information.

2.2 | Overview: Current methods and practices

A number of industry practices and techniques allow online social media and networking users to manage and regulate the nature and amount of personal information that they share online. The industry practices range from incorporating privacy by design into the development and management processes of technologies to providing users with specific options that enable them to manage and control the flow of their online information. On the other hand, technological methods range from data security and encryption services to various online privacy-enhancing technologies. This section provides a brief overview of such practices and techniques in relation to the security and privacy of users' online personal information on social media and OSN services. Broadly, these methods and practices are currently of three types:

- Taking user consent and providing them with privacy options;
- Using data encryption and anonymization techniques for data security; and
- Providing users with privacy-preserving online technologies such as distributed social networks.

a) User consent, privacy options, and do-not-track

The primary industry practice that enables online social media and networking services to collect, store, and process users' personal information is the use of explicit agreements between the online service provider and the user. This is done by making sure that users can only use these services if they agree to the Terms and Conditions (T&C) and the privacy and

data use policy of the website. Such an agreement depends explicitly on user consent and is widely used across all major websites and online services including Google, Facebook, Pinterest, Twitter, Hvyes, and Spotify. However, such an approach based on user consent faces two major difficulties concerning the privacy and security of users' online information:

- The T&C and privacy policies are often lengthy and contain technical and legal jargon making it difficult for users (especially minors and young children) to fully read and understand them; and

- The users need to fully comply with the T&C and/or the privacy and data use policy of an online service to be able to use it. If a user disagrees with a specific clause within the policies he/she still needs to accept and agree to the entire policy in order to use the web service, thereby forcing users to sometime accept invasive and often intrusive T&C.

Apart from user consent on information collection and processing, online social media services and OSNs also provide users with a set of options to control and regulate the nature and content of the information that they share on these sites. These settings are either explicitly provided to the user or are part of the broader profile and account settings on social media and networking websites. These settings (and their default values) vary across different websites. However, as indicated earlier in section 2.1.a, users often face difficulties in using the settings provided by such websites (King, Lampien, & Smolen, 2011). Moreover, often these settings do not provide a granular level of control over online data management and thus restrict the ability of users to manage and control their information on various online services (e.g. Christofides, Muise & Desmarais, 2009; FTC, 2012b; Hull, Lipford & Latulipe, 2011; Krishnamurthy & Wills, 2008; Lewis, Kaufman & Christakis, 2008).

Apart from the practice of taking user consent and providing privacy features, an important upcoming industrial practice is that of Do Not Track (DNT).[15] DNT is an online mechanism through which users can selectively opt out of third-party online user data tracking including that done by search engines, and social media and networking sites, as well as the tracking done for the purposes of gathering online analytics. This technology is based on the existing web standards and is fully compatible with the current state of the Internet. However, user tracking is an integral part of online advertising and in this regard DNT remains an ineffective solution. DNT does not allow for granular user control over information, relies entirely on users' awareness of this option, and is generally not followed by most advertising companies or publishers owing to their commercial interests (see, for e.g. Meyer, 2012; Weinstein, 2012).

[15] Refer: http://donottrack.us/

b) Data encryption and anonymization

The information gathered by online social media and networking technologies is often stored in an encrypted format to prevent unauthorized access and modification.[16] Data encryption is a technique in which a particular piece of information is encoded in a specific format, making it unreadable to anyone without the encryption key. A number of data encryption algorithms and standards are used online such as the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), and the Advanced Encryption Standard (AES). In addition to the encryption of stored data, an industry standard used for the encryption of information communication between parties online is the Hypertext Transfer Protocol Secure (HTTPS). HTTPS is a communication protocol that provides the means to securely transmit information online. Almost all major social media and networking sites, including Facebook and Google+, provide users with the option to use their services using the HTTPS protocol to protect unauthorized access and online phishing[17] of their personal information.

Moreover, a number of techniques are now being developed to provide differential privacy as well. Differential privacy refers to the privacy of information which is mined from large datasets. For example, government records of user information are usually stored in large databases which have to allow for data mining for research and statistical purposes. However, within these processes of data querying, there is also a need to protect the privacy of individual records in order to prevent identification of particular persons and legal entities. This is done by using differential privacy algorithms. Although these techniques are part of standardized industry regulations and policies, research has shown that encrypted and anonymized data can still reveal particular patterns (Backstrom, Dwork, & Kleinberg, 2007). Moreover, other research has shown how data on online social networks and other public sources can indeed be used to reveal users' personal and sensitive information such as social security numbers (Acquisti & Gross, 2009).

c) Privacy-preserving and enhancing mechanisms and technologies

A number of privacy-preserving and enhancing technologies (PPETs) have been created not only to provide users with alternative online services in place of mainstream applications but also to enable users to further monitor and regulate the nature and content of the personal information that they share online. PPETs can be understood as ways and tools which allow users to access, regulate, and monitor not only the information that they explicitly share online but also the data that first- and third-party trackers and widgets gather on their online activity. PPETs are of various kinds including, but not limited to:

- Using multiple email accounts for specific purposes thereby distributing your information across multiple non-consolidated profiles;

[16] See for example Google's (http://www.google.com/policies/privacy/) and MySpace's (http://www.myspace.com/Help/Privacy?pm_cmp=ed_footer) data use and privacy policies.

[17] Phishing refers to the illegal act of acquiring users' personal information by pretending to be someone else

- Multiple users using a single account to access a particular web service or application thereby preventing single user profiling;
- Using online proxies to anonymously interact with websites and services;
- Providing incomplete or false information on online web services and applications. It must be noted here that providing false information is deemed an illegal activity within the T&C of online social media and networking services. However, certain government and non-government agencies advise social media and networking users to provide incomplete or even false information to web services in order to protect their privacy. For example, a senior UK government official recently sparked a controversy by advising users to provide false details to social networking organizations (Wheeler, 2012); and
- The use of specific browser add-ons/plugins to regulate the information shared between the user's device and online services. Examples of these include: AdBlocker and Ghostery.

An important example of privacy-preserving technologies is a Lockr system. Lockr allows users to control the privacy loss on their own social information by decoupling the social networking information from other OSN functionality using social attestations, which act like capabilities (Ganjali, Saroiu, Tootoonchian, & Wolman, 2009). These social attestations are used for authentication and authorization is enforced using separate authorization policies. Persona uses attribute-based encryption to realize privacy-preserving OSNs. The attributes a user has (e.g., friend, family member, colleague) determine what data s/he can access. The NOYB approach adopts a novel approach for preserving content privacy (Francis, Guha & Tang, 2008). They observe that if users address their privacy issues themselves by hosting encrypted content on OSNs, they could be expelled from the OSN by the OSN operator. Hence, they propose to replace users profile content items with ``fake'' items randomly picked from a dictionary. NOYB encrypts the index of the user's item in this dictionary and uses the ciphered index to pick the substitute. On the other hand, flyByNight encrypts the users' content that hosts on the OSN (Borisov & Lucas, 2008).

Moreover, an important class of online social media and networking privacy-preserving technologies is that of Distributed Social Networks (DSN). A DSN is an online social networking service which consists of multiple websites running simultaneously to provide decentralized means of large-scale communication across website users. For example, the distributed social networking service Diaspora has 132 installations and provides services to approximately 350,000 users (Diaspora Alpha, 2013). These installations can communicate and interact with each other, providing users with a virtual environment in which users' personal information is not stored and processed at one centralized location but instead it is distributed across multiple locations and installations. DSNs are also sometimes referred to as

federated social networks. Oft-cited examples of DSNs include Diaspora,[18] buddycloud,[19] and BuddyPress.[20]

Compared to mainstream OSNs such as Facebook, MySpace, and Google+, DSNs have certain advantages regarding the privacy and security of users' online personal information:[21]

- DSNs provide greater control over what information is collected, recorded, and processed within the social network;
- DSNs provide granular privacy settings, facilitating explicit and detailed user control over the nature and content of information that users wish to share;
- DSNs allow users to install new features (via scripts) as and when required; and
- Since DSNs allow users to control the flow and processing of their information, these networks also help minimize third-party tracking and targeted advertising practices.

DSNs mostly use freely available open standards within their implementation. An open standard can be understood as a publicly available standard that provides users with specific means for performing a particular task. For example, the OpenID standard identifies ways in which online users can be authenticated using decentralized means.[22] An implementation of this standard (such as in Google, VeriSign, and myOpenID) can then be used by online services to facilitate user authentication within and across applications and services. Other examples of distributed social networking open standards used by DSNs include Tent, OAuth, OpenSocial, and a group of open standards and protocols collectively referred to as the Open Stack.

Recently, the issue of using decentralized infrastructures for organizing OSNs in a privacy-preserving manner was addressed by the research community. PeerSon adopts encryption mechanisms for content storage and access control enforcement. It uses a two-tier architecture in which the first tier is a DHT, which is used as a common storage by all participants (Buchegger, Datta, Schioberg & Vu, 2009). The second tier consists of peers and contains the user data. The DHT stores the meta-data required to find users. Peers connect each other directly, exchange the content, and then disconnect. The work by Cutillo, Molva, & Strufe (2009) addresses privacy in OSNs by storing profile content in a P2P storage infrastructure. Each user in the OSN defines his/her own view (*matryoshka*) of the system. In this view, nodes are organized in concentric rings, having nodes at each ring trusted by the nodes in its immediate inner ring, with the user node being the center of all rings. The user's profile data is stored encrypted at the innermost ring, which is accessed by other users through multi-hop anonymous communication across this set of concentric rings. In the DHT, an entry

[18] Link: https://joindiaspora.com/

[19] Link: http://buddycloud.com/

[20] Link: http://buddypress.org/

[21] For a detailed analysis of the comparison between the features of existing DSNs and user requirements, see Thiel et al. (2012).

[22] Refer: http://openid.net/specs/openid-authentication-2_0.html

for a user with the list of nodes in the outermost ring is added. Thus, this approach achieves both content privacy (using encryption) and anonymity of searcher and hosting nodes, yet limited content discovery and profile availability.

A decentralized OSN, Vis-`a-Vis is proposed in the work done by C´aceres, Cox, Shakimov & Varshavsky (2009), where a user's profile content is stored at his/her own machine called as virtual individual server (VIS). VISs self-organize into P2P overlays, one overlay per social group that has access to content stored on a VIS. Three different storage environments are considered – cloud alone, P2P storage on top of desktops, hybrid storage – along with an analysis of their availability, cost, and privacy trade-offs. In the desktop-only storage model, a socially-informed replication scheme was proposed, where users replicates their content to their friend nodes and delegate access control to them. However, normally users trust only a fraction of their friends to the extent of delegating access control enforcement.

Tribler is a P2P file sharing application which exploits friendship relationships, tastes and preferences of users to increase the performance of file sharing (Bakker et al., 2008). However, in Tribler, users host their own profile and therefore profile placement for high availability and low access or consistency cost are not considered. Finally, LifeSocial is a P2P-hosted OSN where users employ public-private key pairs to encrypt profile data that is stored in a distributed way and is indexed in a DHT (Graffi et al., 2009). Friends can read a user's profile based on a symmetric key that is encrypted with their public keys. However, data privacy and profile availability are not considered in the work done on LifeSocial.

The researchers in the Replica project pursue the notion of online times for a P2P client in detail. Various replica placement strategies are studied analytically. The Diaspora project aims to build a user- owned decentralized online social network. It consists of independently owned *pods* (or servers), which host user profiles and form the network. However, the Diaspora system needs the pods to be online always. Finally, My3 is a decentralized OSN with no requirement on nodes being online that focuses on certain performance aspects of the system that make it practically attractive for users, such as high profile availability, low profile update delay, low access delay and high privacy (Aberer, Narendula & Papaioannou, 2012). My3 proposes different replication strategies towards the different performance objectives and allows content searchability by employing a privacy-preserving index.

2.3 Mobile devices, Location-Based Services, and User Privacy

Mobile devices, such as smartphones and tablets, contain a large volume of users' personal and sensitive information such as their contacts, photos, messages, and videos. Moreover, these devices are quite unique, compared to traditional computing devices such as desktop computers, in that mobile devices are often carried by users wherever they go. Thus these devices can track, gather, and store information about users' geolocation data history and

daily routines such as the usual route that a user follows to work.[23] Smartphones and tablets also enable users to install and use a host of mobile applications (usually referred to as 'apps') through mobile app-stores such as Apple's App Store and Google Play. These first- and third-party mobile apps often use the location sensor in these devices to identify a user's approximate location at a given point in time in order to provide specific services such as searching for a restaurant nearby. Figure 8 depicts the results of a study done by Microsoft concerning user awareness of location-based mobile services and related privacy concerns.

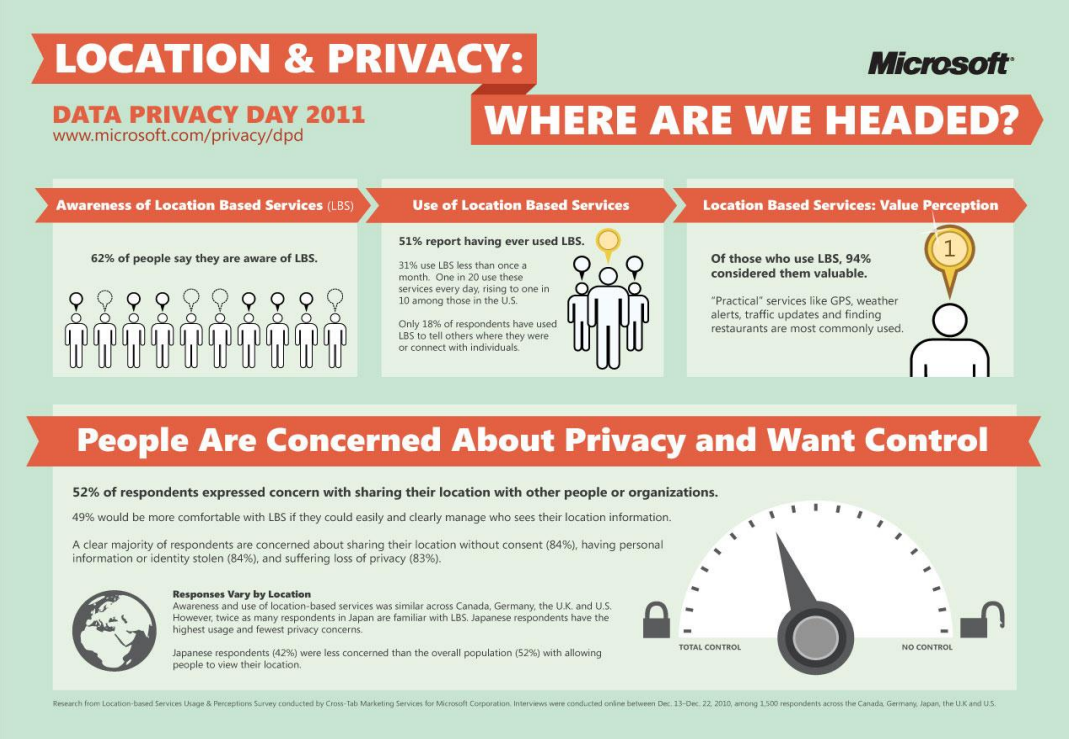


Figure 8: Location and Privacy – Microsoft Infographic [24]

Owing to such characteristics of mobile devices, these devices raise a large number of issues and concerns in relation to the privacy and security of users' personal information. Figure 9 displays an infographic depicting the results of a study which highlighted that mobile users are significantly concerned about the privacy and security of their mobile information. Broadly, the existing and plausible issues and concerns concerning the privacy of users' personal information on mobile devices fall within two categories:

- Location-based services and data convergence; and
- Big Data and user privacy issues and concerns.

[23] For example, this particular ability to record and monitor users' daily routines is an essential part of Google's new technology called Google Now (http://www.google.com/landing/now/) – a virtual mobile assistant available on Google's android devices.

[24] Source: http://www.microsoft.com/en-us/news/features/2011/jan11/01-26dataprivacyday.aspx

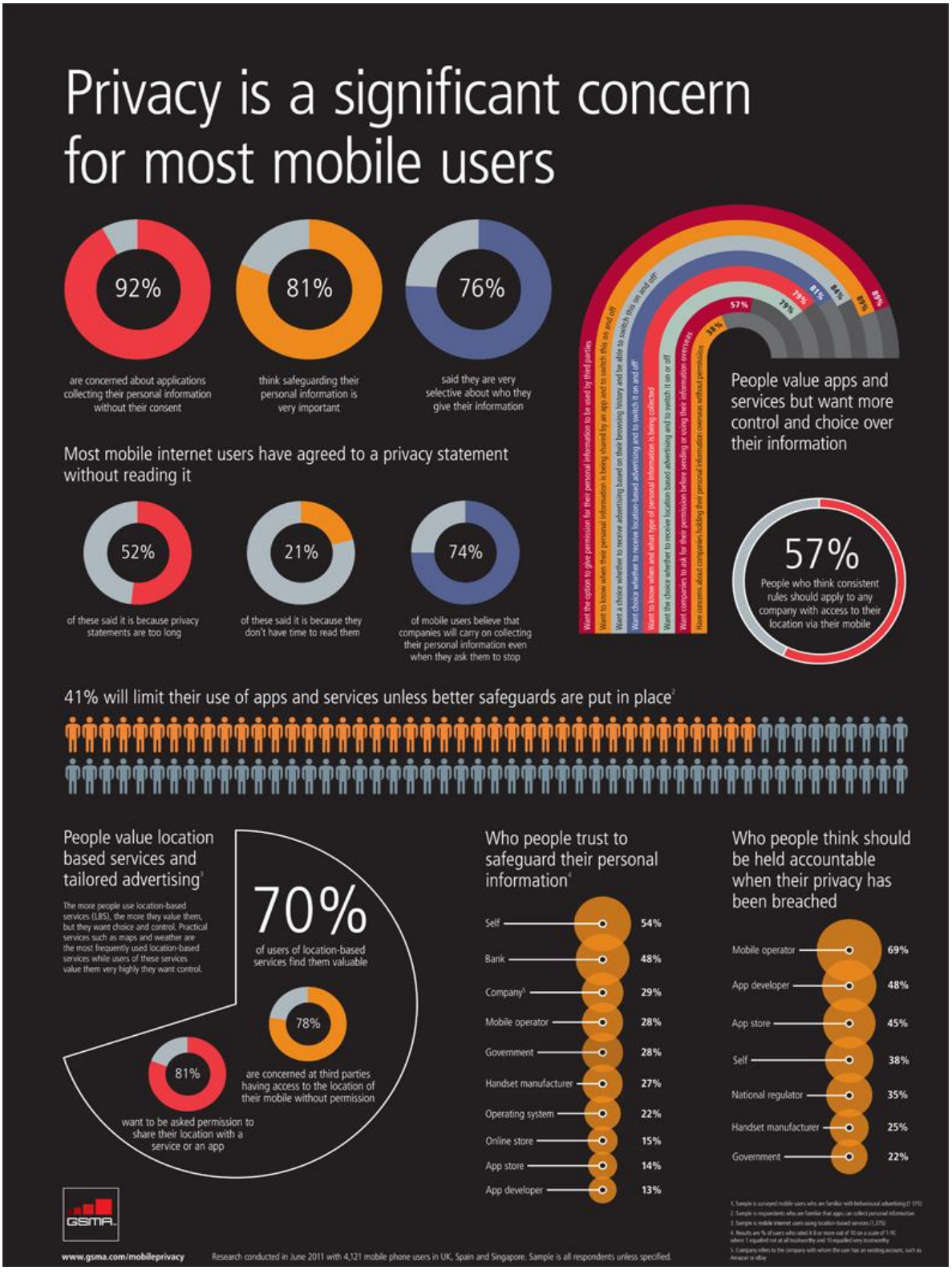


Figure 9: Mobile users are concerned about information privacy [25]

a) Location-based services and online/offline data convergence

[25] Source: http://www.gsma.com/publicpolicy/privacy-infographic

With the widespread diffusion of mobile devices, location-based services are increasingly becoming more popular. Location-based services are application services that employ users' geographical location data to enable and facilitate user search for particular items, to track specific objects, or to allow companies to target specific advertisements towards users at a particular location. Common examples of the use of mobile location-based services include:

- Searching for a restaurant or pub near one's location;
- Playing location-based games such as Geo-Tags; and
- Sharing one's location by checking-in at a particular location.

In addition to enabling and facilitating particular features and applications, location-based services also raise a number of user privacy and security concerns. This usually happens when location-based services (such as Foursquare) are used in conjunction with other social media and networking services (such as Facebook) to develop social discovery applications. Social discovery applications can be understood as services that allow users to search for and discover other social media and OSN users either close to their own location or close to a specific location elsewhere. Figure 10 shows two oft-cited examples of privacy-invasive social discovery as well as social networking mobile applications.

Figure 10: Examples of privacy-invasive social discovery mobile apps

The first is the Girls Around Me app which was released on Apple's App Store in 2012. Through this app, a person could search around his/her location for nearby girls. The app took

public data from Foursquare and coupled it with the public images of girls on Facebook to provide the user with an interactive map displaying a comprehensive visualization of information pertaining to girls around his/her location. Although the app was subsequently taken down, this example clearly depicts how third-party social applications can have consequences for societal notions of privacy and trust by facilitating novel means of large-scale tagging, identifying, and converging not only online information but also the exact locations of mobile users. The second example is that of 'Badabing' – a mobile app that allows a user to search through his/her Facebook friends' online photographs to reveal the friend's semi-nude pictures. Although Badabing is not a location-sensitive app, it illustrates how social platforms can indeed be used in innovative and non-traditional ways to search and manipulate information within existing social media and networking services through the use of social platform APIs.

An in-depth understanding of public and private contexts in relation to characteristics particular to the mobile medium provides a relevant point of entry to examine such privacy and security issues. Although Facebook photos and Foursquare check-ins might have separately been made public by certain users, the combination of the two coupled with an exact location on the map is certainly not what users explicitly consented to. By identifying and merging particular bits of scattered information, apps such as 'Girls Around Me' facilitate the collapsing of public and private contexts and pose a substantial threat not only to an individual's privacy and personal security but also to socially acceptable forms of data mining.

Moreover, although such apps can be regulated on standardized app-stores provided by Google or Apple, the ease of working with social and mobile platforms makes it increasingly difficult to manage and govern the intentionality of the large number of mobile apps that are developed each day. Social networks and mobile devices have now become ubiquitous tools that are used by individuals to manage their everyday lives and mobile app development has become a substantial market in itself. In such a scenario, it is imperative to examine the implications of the ability of third-party applications to facilitate the large scale convergence of user information in ways that are quite novel and non-traditional.

b) Big data and user privacy

Business organizations and companies now use large-scale data gathering and processing mechanisms not only to ensure the proper working of their services and applications but also to help them manage and innovate existing services and business practices. In this regard Big Data is increasingly gaining importance within market research as well as in relation to user studies and service and management innovation. Big Data can be understood as a collection of multiple datasets containing a very large volume of information pertaining to, for example, business practices, user behavior, health and medical records, and income tax data. Big Data is a contemporary phenomenon and market research firms and information scientists are working to find and develop further applications of such large datasets. Social media and OSNs are prime examples of Big Data in which information predating to large number of

users – across multiple web services and applications – is stored. Figure 11 depicts an infographic explaining the heuristics of Big Data.

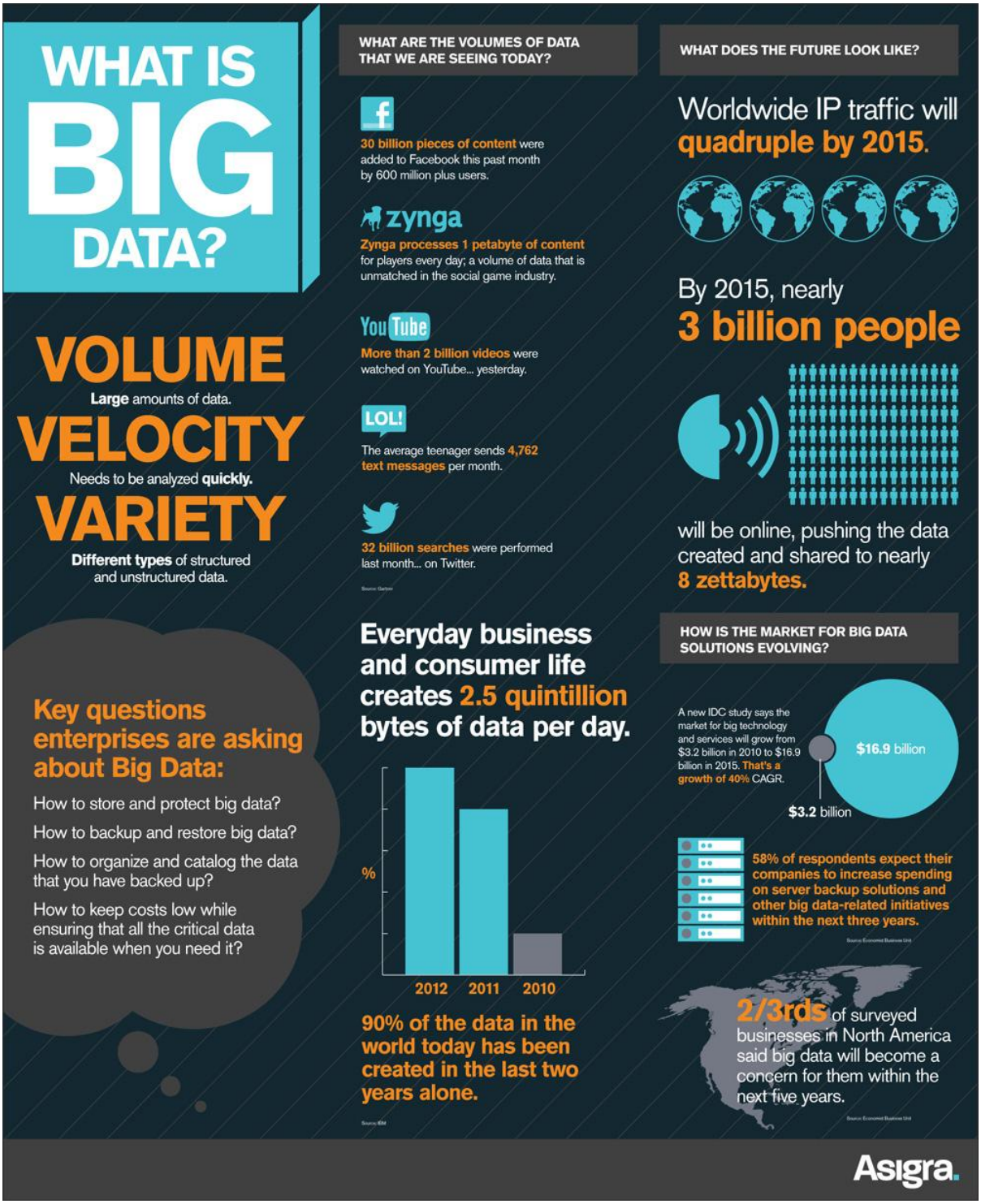


Figure 11: Understanding Big Data [26]

[26] Source: http://www.asigra.com/blog/big-data-infographic-what-big-data

However, such large datasets also pose substantial privacy and security risks pertaining to users' personal information such as health and medical records as well as in relation to government records. Moreover, with the advent of online social media and networking services, online organizations now possess a large volume of information such as users' personal information, browsing and search histories, ecommerce transactions, as well as user activity across multiple third-party web services. Such detailed user profiling raises a host of privacy issues as explained earlier in section 2.1. These datasets can then be processed in different ways to correlate and contrast information across multiple users and web services. This can lead to privacy-invasive applications of Big Data (Chew, Balfanz & Laurie, 2008). For example, social media and networking information in conjugation with publicly available data can be used to predict users' social security numbers (Acquisti & Gross, 2009) amongst other things (Bonneau, Anderson & Danezis, 2009).

It is clear that Big Data have great potential for market research and innovation; however, at the same time such large datasets also raise privacy and security concerns. Research has shown that even anonymized data within large datasets can be processed in ways so as to reveal the true identity of the data subject (Backstrom et al., 2007; Srivatsa & Hicks, 2012). Moreover, these datasets can be further exploited to reveal a substantial portion of a user's personally identifiable information (Le Blond, Zhang, Legout, Ross & Dabbous, 2011). The contemporary turn towards Big Data thus necessitates further research into not only the possible applications of Big Data but also ways to ensure the privacy, security, and anonymity within large datasets.

3. Privacy and Behavior/Conduct

This section deals with social behavior and conduct issues concerning privacy, trust, reputation, and identity on the Internet, particularly in relation to the use of online social media services and OSNs. Section 3.1 examines the social norms and practices concerning the use of OSNs, including themes such as online identity formation, social norms and practices of sharing information online, and contextual integrity regarding online user information. Section 3.2 focuses on the use of social media by children and teenagers, especially issues of social network privacy, trust, reputation, and identity.

3.1 | Social Norms and Contextual Integrity

Different people interpret, interact, and use online services and applications differently. Digital technologies provide novel means of large-scale interpersonal communication. When users appropriate digital technologies such as OSNs they try to use and configure them according to their own needs. While some people use online social media services and OSNs primarily for online identity and network formation, some use them simply as tools for long-distance communication with family and friends. Moreover, OSNs like Facebook are increasingly becoming commonplace within schools and workplaces (DiMicco & Millen, 2007). Nonetheless, although the major uses of online social media and networking sites have not changed much over their short history, users' perceptions of intended audiences and social sharing norms and practices are continuously changing (see Lampe, Ellison, & Steinfield, 2008). Such changes depend upon many factors such as the nature of the relationship between two individuals, the movement of an individual from one place/institution to another, the nature of content that users share online, as well as the social groups and contexts to which the online user belongs.

The particular features of online technologies also shape and influence the way users interact with them. Within this context, the existing social norms and practices concerning interpersonal communication play an important role. The nature of content that a user shares on his/her online profile or communicates to another user depends upon his/her relationship with online social groups and users (Nissenbaum, 2010). For example, a user might want to share a particular piece of information with a specific group of people only and not want other users to access that information. For this, online technologies provide privacy settings that allow users to monitor and regulate the flow of their online information. The way online technologies handle user information and the nature of privacy controls that they allow thus highly influence and constrain the nature of online communication that users can have on such networks. Moreover, people sometimes find it difficult to understand and implement privacy settings on OSNs and many users often underuse (or completely ignore) these privacy settings (Strater & Lipford, 2008). Liu, Gummadi, Krishnamurthy & Mislove (2011) found that even when users do change their default privacy settings, the new settings only match their expectations 39% of the time – clearly indicating that even users who are more privacy-aware have difficulties in managing their OSN privacy. This raises a number of online privacy issues and concerns.

There is a strong correlation between online privacy expectations and offline privacy norms and practices. Thus novel technologies, by changing existing practices of online communication and sharing, often raise a number of user privacy issues and concerns (Martin, 2012). Specifically with regard to the privacy of online information, user privacy expectations and concerns primarily stem from a strong belief in the right to privacy as well as a social and psychological need for online privacy (Yao, Rice & Wallis, 2007). Depending upon the social circumstances and issues, users take a variety of steps to ensure the privacy of their personal online information.[27] For example, a study about OSN privacy management tools found that of the 2277 surveyed adults, 63% had deleted specific people from their friends' list, 44% had deleted comments of other users from their profiles, and 37% had removed their name tags from online photographs (in an attempt) to protect their online privacy (Madden, 2012). The fact that a majority of users prefer to send personal information by private messages and emails instead of on OSNs (Young & Quan-Hasse, 2009) provides another example of online privacy management.

Specifically with regard to informational privacy, people often do not explicitly recognize online privacy issues and concerns and repeatedly provide the 'I have nothing to hide' argument as a response to concerns over the privacy of their online information (Solove, 2007). Within such an interpretation of rights to privacy it becomes increasingly difficult to stimulate users to adopt privacy-enhancing practices and to raise a broader debate about the multiplicity of online privacy issues. The latter include, for example, the problem of identity theft, access of online information by unintended audiences, the use of publicly available information by researchers, and the use of OSNs by minors and young children. Figure 12 depicts the multiplicity of risks associated with the sharing of information online. There are four broad categories of online privacy, reputation, and identity issues pertaining to social norms and behavior:

- A desire for sharing and a need for anonymization;
- Difference between visible/invisible and intended/unintended audiences – and an understanding of privacy issues in relation to sociocultural contexts;
- The paradoxical relationship between privacy and control; and
- Use of publicly available data by researchers.

a) Identity versus anonymization

Online social media service and OSNs are tools for large-scale interpersonal communication and data-sharing, and thus it is in the business interests of online organizations to design these services in such a way so as to enable and facilitate as much user data sharing as possible.

[27] For an overview of the different strategies used by users refer to Lampinen, Lehtinen, Lehmuskallio & Tamminen (2011).

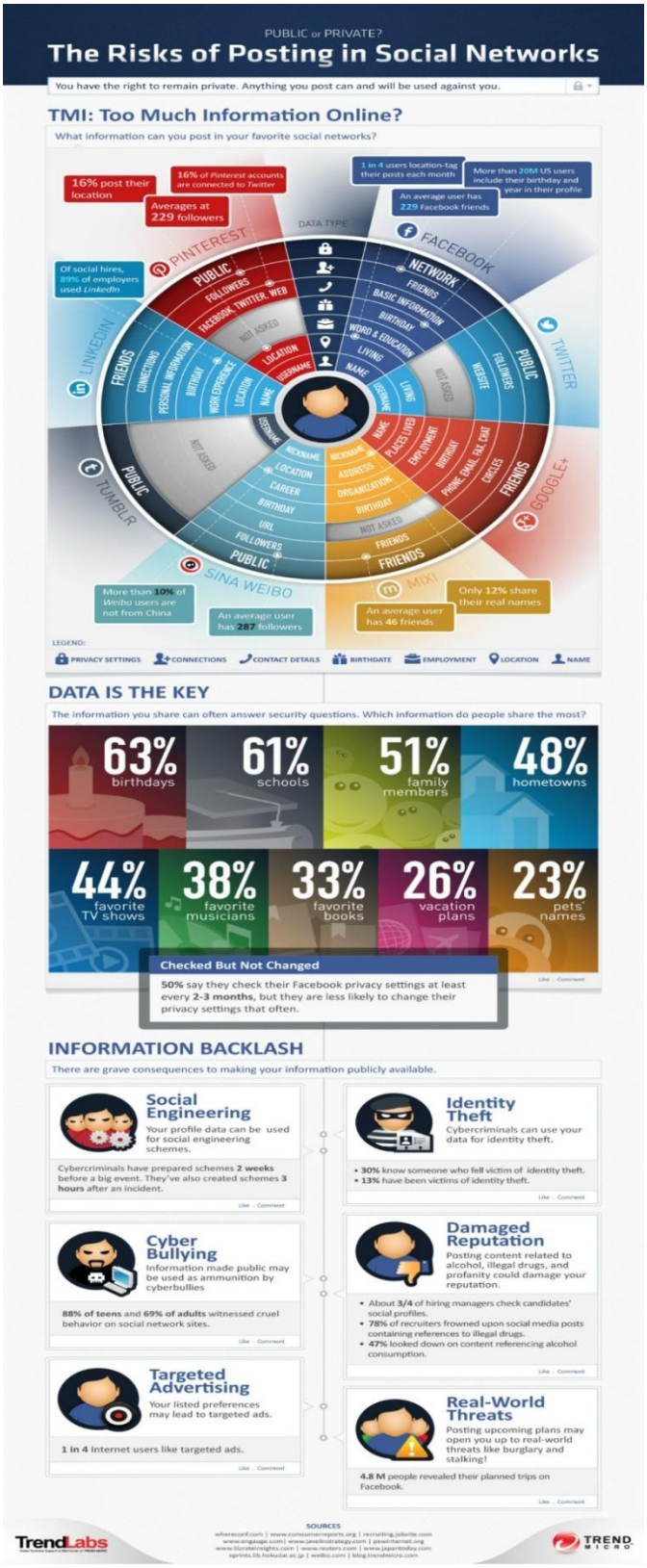


Figure 12: Risks of posting on OSNs [28]

[28] http://mashable.com/2012/09/12/protection-for-social-networks/

However, at the same time sharing personal information online raises a number of privacy issues and concerns, creating a need for greater data transparency and control as well as detailed privacy settings. Users thus find themselves in a place where they have a desire to share personal information as part of their online identity and network formation while at the same time privacy concerns force online users to ensure the anonymity of some of their online information. This contradiction forms the bedrock of a majority of online privacy issues, especially those pertaining to the use of online social media and networking technologies such as Facebook, Google+, and MySpace. In general, people with online social profiles have a tendency to take more risks online especially pertaining to the sharing of personal information and in this regard it has been recommended that OSNs should inform users of potential privacy risks and issues before allowing them to sign up to use their services (Fogel & Nehmad, 2008).

A study done about the level of information that people need to form impressions of other people showed that people not only form major opinions based on online profiles of users but also need only a "thin slice" of users' online profile information to form their impressions (Stecher & Counts, 2008). Moreover, research done on the use of OSNs also shows that often users abandon their own privacy concerns in lieu of generating social capital and networks, and often use their own trust to judge whether a particular piece of information can be shared or not (Trepte & Reinecke, 2011). This observation is further evident from research done on the use of location-enabled mobile devices. The research highlighted three factors that users felt were of prime importance in deciding whether they wanted to give away their location data to other users/parties: a) who wants the information, b) why do they want it, and c) what level of detail is being asked for (Consolvo et al., 2005). Depending upon the answers to these questions, users were more or less willing to share their location data completely.

The conflict between the desire to create and shape one's online identity and the need to remain anonymous plays out within the dynamics of online identity formation. The way in which online identity is formulated and constructed is being reshaped by digital experiences through social technologies. The expansion of realms for identity exploration generates issues of multiple identities and the convergence of digital online identities with offline ones. These changes mean that the ways in which identities are constructed and continually reconstructed through the expansion of digital experiences will inevitably be different. An important development in the privacy domain is the apparent discrepancy between what users say about their online security concerns and their actual behaviors. Evidence indicates that although Internet users express privacy-protectionist views, this rarely translates into behavior and practice (Barnes, 2006; Gross & Acquisti, 2005; Young & Quan-Hasse, 2009). This points towards an important area of enquiry: why is there a significant departure from offline privacy behaviors and how is it that online privacy behaviors are so different?[29]

[29] On the other hand there are also a number of studies that question and/or disprove the online privacy paradox. Refer: Brandtzæg, Lüders, & Skjetne (2010); Krasnova, Spiekermann, Koroleva, & Hildebrand (2010); and Staddon, Huffaker, Brown, & Sedley (2012).

Many users exhibit "functional illiteracy" when it comes to privacy-protecting technologies (Carey & Burkell, 2009), suggesting that users in digital social environments may have difficulty imagining the kinds of harm that could arise from putting personal information online. The decline of anonymity is also in part due to visual, facial searches where faces become links between online and offline data. The potential of "Personally predictable information" was highlighted in Acquisti's Face Recognition Study (2011).[30] The implications are far reaching if from just one piece of anonymous information, a person's face, additional sensitive data about the person can be extrapolated. This highlights the nature of online privacy concerns arising from the growing desire users have to create and shape their online identities while at the same time trying to find appropriate limits to data sharing so as to preserve the privacy of their online information.

b) Visible/invisible and intended/unintended audiences

A distinct feature of online information, especially on online social media services and OSNs, is that it enables and facilitates a one-to-many communication pattern. Information shared by one user can simultaneously be accessed and read by multiple users. Moreover, a large volume of online information shared by users can also be accessed and read by online organizations and other third-parties. Within this context, an important privacy concern for online users is the difference between visible and invisible audiences. The gathering, storing, assimilation, and processing of users' personal information by invisible audiences, groups about which users are not explicitly aware of, can lead to online privacy issues. This is the case with the Facebook-Datalogix partnership as well as the privacy issues concerning the use of invisible online trackers, widgets, and beacons.

Another important distinction concerning online user privacy is that between intended and unintended audiences. Users often share information with a particular target audience in mind. In this regard, OSNs provide privacy settings that enable users to target their content to specific groups of people. The 'smart group' feature on Facebook and the Circles feature on Google+ are prime examples of this approach. Smart groups (and Circles) allow users to segregate their online friends into various groups, each with its own privacy settings and dedicated OSN space. However, although these features provide mechanisms to regulate the sharing of online user information, the inability of such technological features to accurately mimic social norms and practices of everyday communication is often targeted by online privacy advocates as well as digital media researchers (Van den Berg & Leenes, 2010). Critics also argue that users increasingly find it difficult to interact with and use such privacy mechanisms (Lewis, Kaufman & Christakis, 2008; Livingstone, Ólafsson, & Staksrud, 2011) and the fact that online organizations keep changing and adding new features and mechanisms makes it increasingly difficult for end-users to effectively manage their online privacy.

An oft-cited example of this was the launch of Facebook's News Feed and Mini-Feed feature in 2006. News Feed provided a dedicated online space in which the information shared by a user's friends was assimilated onto one single page (and within the Mini-Feed in

[30] See: http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/

the sidebar). There was a huge outcry when this feature was launched, and a vast majority of users raised their concerns over the privacy-invasive nature of information that was in fact already public (boyd, 2008a). The only difference from the already existing features was that the information was gathered and put in a single, easily accessible place. Such incidents illustrate that people sometimes become concerned about privacy. People share information with particular audiences in mind and when such information is featured across all users' News Feeds it can lead to perceptions of privacy invasions in the form of easier informational access and loss of control over one's personal information (Hoadley, Xu, Lee & Rosson, 2010). A vast majority of online users counteract such difficulties by keeping a friends-only profile on online social media and networking services (Stutzman & Kramer-Duffield, 2010).

c) Paradoxical relationship between privacy and control

Another major online privacy concern is the paradoxical relationship between privacy and control: the strong correlation between users' perceived control over their online information and the amount of information that these users share online. It has been shown that people with a large number of friends often tend to share more information online (Young & Quan-Hasse, 2009). Moreover, there also exists a correlation between keeping one's online profile private and a higher level of online activity: people with private profiles do share and communicate a lot of information online (Lewis et al., 2008). This is also true for OSNs that provide users with a large number of privacy options and settings. When users feel that they can monitor and regulate their information in a detailed manner, they tend to share more personal information on such social media and networking services (see, for example Barnes, 2006; Gross & Acquisti, 2005; Radin, 2001).

d) Researchers and publicly available user information

Online social media and networking sites often contain vast amounts of publicly available information pertaining to a large number of users. This provides a rich data source for researchers to gather, collect, and process data from. However, there are a number of legal and ethical issues pertaining to the use of such online data for academic and industry research purposes (Wyatt, 2012). An oft-cited example of this was the release of a Facebook dataset comprising information about a group of US college students in 2008. Although a number of attempts were made to hide the true identity of data subjects and the university, the true source of the data was quickly uncovered, exposing students to online privacy risks and issues (Zimmer, 2010).

Often industries also use online user information for research purposes either to improve their own service designs or to develop new applications. Thus, these industries need users who are willing to be profiled and to share their information with them. Thus these firms need to emphasize issues such as data transparency. However, research has shown that often users who value and desire greater online data transparency are the same users who are far less willing to be profiled online (Awad & Krishman, 2006), presenting a paradox for these firms. In this regard there is a need to create more efficient privacy-preserving data collection, storage, and processing mechanisms so as to prevent unintended privacy issues and concerns over the use of certain publicly available datasets for research purposes.

3.2 | Young People and Privacy

Many children and young teenagers are increasingly making their own online presence especially on social media and networking sites. This is evident from the results of a large-scale survey done within the EU Kids Online project covering 25 European countries and 25,000 respondents. The results of the survey indicate that in Europe nearly 80% of 13-16 year olds and approximately 40% of 9-12 year olds have an online profile (Livingstone, Olafsson & Staksrud, 2011). Although several OSNs ban minors (children below the age of 13) from using their services, the report indicates that in the absence of reliable age-verification techniques under-age users are also prevalent on OSNs. Moreover, a substantial portion (57%) of 9-16 year olds who have an online profile primarily use Facebook and a large proportion of these users have their privacy settings set to 'public'.

Youngsters often exercise control over the sharing and communication of their online personal information by using privacy settings, employing nicknames, and blocking specific people instead of restricting the amount of information that they reveal and share online (Tufekci, 2008). However, the results of the EU Kids Online survey also indicate that these privacy features (such as privacy settings and the ability to block a particular user) are not easily understood and used by many youngsters and children in European countries. Such difficulties in interacting and using the privacy settings on social media services and OSNs, not only in Europe but also in the USA and Canada, often result in some children not using such settings at all, leading to undesirable outcomes. For example, a number of young girls have either been sexually harassed or assaulted through online social media and networking services (Cassell & Cramer, 2007).

Thus, children face a host of online privacy issues and threats including, but not limited to, sexual abuse, location tracking, cyber bullying, and online scams. Figure 13 depicts the nature of cyber-bullying. A number of young online users have also reported meeting a complete stranger whom they first encountered online (Liau, Khoo & Ang, 2005). With more and more youngsters now adopting online services, it becomes essential not only to review how children use and interact with online social media and networking services but also to analyze how the usability and design of such websites enables or restricts children from successfully using privacy mechanisms and settings.

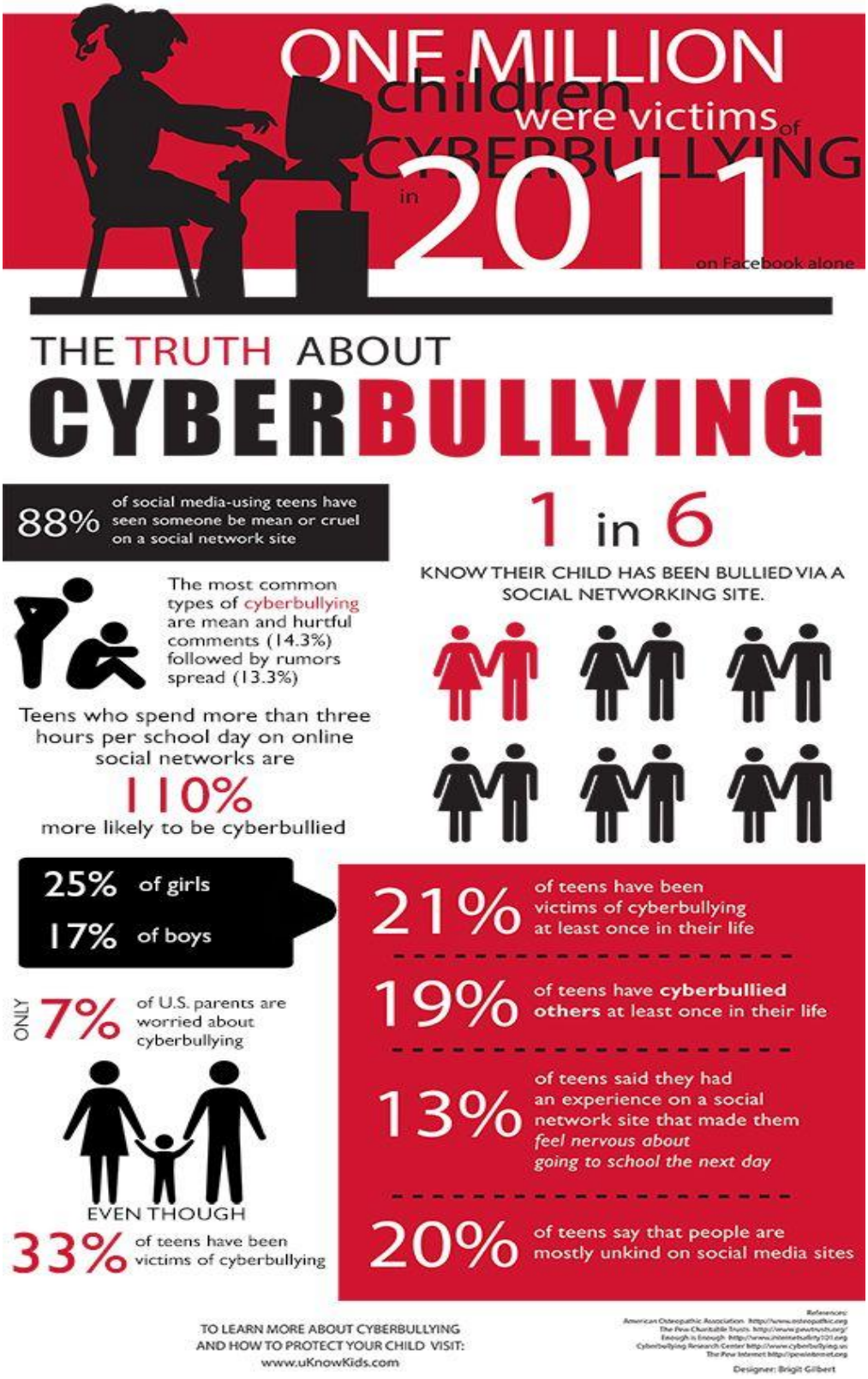


Figure 13: Online Cyber Bullying [31]

[31] http://www.mnn.com/sites/default/files/user-35/CYBERBULLYING_infographic.jpg

With regard to the use of online services by children, three factors are of prime importance:

- The difference between adults and youngsters online;
- The use of online services by children under parental guidance and supervision; and
- Intended audience and collapsing context.

a) Difference between adults and youngsters

Owing to the substantial and prevalent use of online social media and networking services by youngsters, it is a popular conception that minors and young online users have a tendency not only to take more risks online but also to share more personal information online. This has led to a popular belief that young online users are in fact not concerned about their online privacy at all. However, studies show that youngsters not only have a good understanding of online privacy risks and concerns but also often have the same outlook towards such issues as do adults (Hoofnagle, Jay, Li & Turow, 2010). In fact, a study done on 2423 MySpace profiles in 2006 (and follow-up research in 2007) indicated that a vast majority of youth not only limit the visibility of their online profiles but also employed discretion in sharing and communicating online (Patchin & Hinduja, 2010).

Nonetheless, the belief that youngsters care less about their online privacy is not completely unfounded. Although young online users do care about their online privacy (see, for example, Acquisti & Gross, 2006; Gross & Acquisti, 2005), studies based on the usability of online social media and networking sites show that there is a mismatch between users' expectation of privacy settings and the actual outcome of using such services (Strater & Lipford, 2008; Liu et al., 2011). A study done in 2006 showed that young people who are concerned about OSN privacy not only reveal a large amount of their personal information online but also are unaware of the visibility levels of their own profiles on OSNs (Acquisti & Gross, 2006). Such discrepancy between what youngsters say and what they actually do online raises a host of privacy issues and concerns. Furthermore, minors and youngsters are often more concerned about their social privacy (for example, which of their friends get to see their online posts) and far less about the collection, storage, and processing of their personal information by online organizations and governments i.e. informational privacy (Raynes-Goldie, 2010). This, coupled with the difficulty faced by young users in using the privacy mechanisms on a website, exposes them to substantial privacy risks and threats.

b) Children's privacy and paternalism

One of the most straightforward and dominant ways of monitoring and regulating children's use of online social media and networking technologies is parental supervision. Adults have the capacity to better understand the privacy policies and T&C of online services in comparison to children, and thus parental monitoring helps to minimize the threats that children face online. Parental regulation acts as a passport for young users to interact within online services. The EU Kids Online survey reported that 32% of parents do not allow their children to have an online profile and 20% allow them to use OSNs only with supervision

(Livingstone et al., 2011).[32] Figure 14 depicts information provided by parents concerning the use of Facebook by their children.

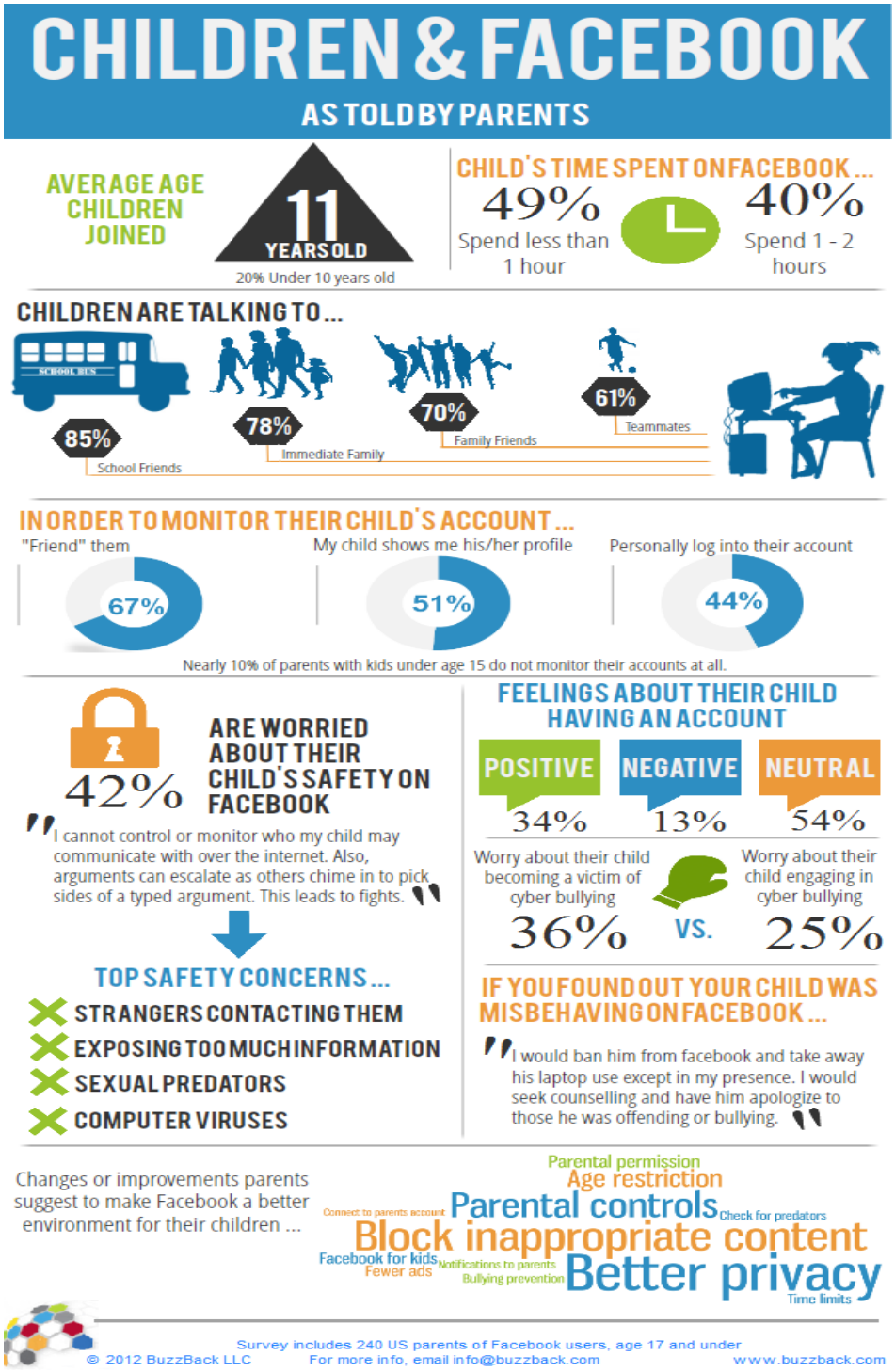


Figure 14: Children's use of Facebook [33]

[32] For detailed information pertaining to parental supervision and children's use of online services, see the publications arising from the eGirls project (http://egirlsproject.ca/), the Young Canadians in a Wired World project (http://mediasmarts.ca/research-policy), and the EU Kids Online project.

However, such an approach faces enormous difficulties. Firstly, minors and young adults rarely add their parents as friends on OSN sites and in general do not want their parents to monitor their online activity as this could lead to social embarrassment, and may be experienced as overly protective or interfering (West, Lewis & Currie, 2009). This creates tensions between children and parents, and teenagers often go ahead and make an online profile even against the wishes of their parents (Livingstone et al., 2011). Secondly, not all parents regulate their children's use of online services. In the EU Kids Online survey, only 50% of parents indicated that they do not restrict/monitor the use of OSNs by their children (Ibid.). Thirdly, research has indicated that most of the young users' coping strategies associated with the risks of the Internet (for example, ignoring or sharing inappropriate content) tend to exclude adult involvement (Staksrud & Livingstone, 2009).

c) Intended audience and collapsing contexts

The notions of public and private are often fuzzy on online social media and networking sites, and youngsters often conceive of the public as their own private online world (West et al., 2009). Such an outlook lends insights into nuanced and novel conceptualizations of the traditional public/private dichotomy on online social media and networking services. By providing overarching privacy group (such as friends, friends of friends, and public), most OSNs collapse multiple audiences into unified contexts (boyd, 2008b). Whereas offline social norms and practices allow people to maintain unique relationships with particular individuals, online services hamper/alter such norms by joining together multiple users in a single group.

This leads to the problem of collapsing contexts wherein a particular piece of information shared for a specific intended audience may also be received and read by other people. Such collapsing contexts may create possible privacy concerns for youngsters, such as the parents of a young girl reading her private online journal and a child's friends harassing him/her online over a tweet/post that was written for a particular person. Although a number of OSNs now provide users with the option to create customized groups, as we have already explained, minors and youngsters not only face difficulties with such mechanisms but also sometimes completely ignore them.

Furthermore, research has shown that often users share and communicate their personal health and medical information on OSNs such as MySpace. A survey of 142 online profiles of 16- and 17-year olds revealed that almost a quarter of users shared their sexual activity (21%) as well as alcohol use (25%), and nearly all of the users (97.2%) shared personal identifying information with 74% profiles containing personal photographs (Moreno, Parks, & Richardson, 2007). Sharing of such personal information online indicates the broad conceptualization of 'public' and 'private' that youngsters usually operate on. Moreover, as explained earlier, with more and more children now using mobile devices the boundaries between public and private blur even further. Mobile devices, coupled with their location-sensing capabilities, enable online and offline data convergence, leading to scenarios in which information intended for specific purposes is used otherwise (such as in the app Girls Around

[33] http://thumbnails.visually.netdna-cdn.com/children--facebook-as-told-by-parents_50a693c00ac65.png

Me). In this regard, figure 15 depicts the results of a survey done on the use of smartphones by minors and young children.

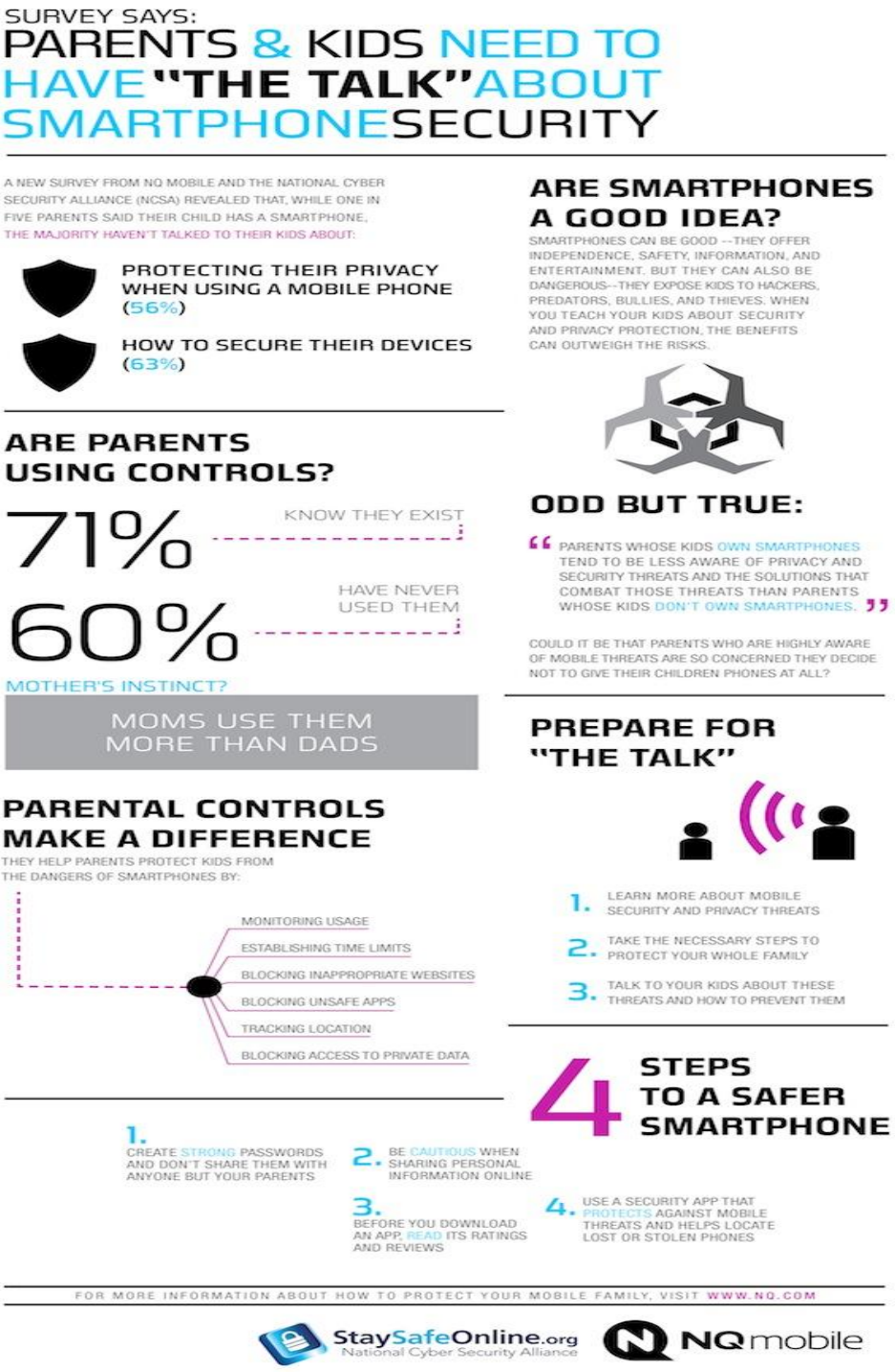


Figure 15: Parents, Kids, and Mobile Phones [34]

[34] http://www.mobile-ent.biz/_media/images/nqmobile_infographic_FAMILYSURVEY.jpg

4. Privacy and Policy

This section focuses on information and data privacy policies, regulations, and authorities (4.1) and on the multiplicity of challenges that information and data privacy policy makers face in the wake of rapidly evolving OSNs and privacy-invasive mobile applications (4.2). Section 4.1 provides an overview of information and data privacy policies, regulations, and authorities within specific European countries, USA, and Canada.[35] These laws and regulations deal not only with the privacy of users' personal information but also with the ways in which industrial and governmental organizations can gather, retain, process, and discard users' personal information. This section also deals with the proposed recommendations within the newly drafted EU Data Regulation concerning the privacy and processing of online user information. Section 4.2 examines the nature of concerns and challenges within policy-making regarding the processing of users' personal and online information by social media technologies.

4.1 | Overview: Information and data privacy regulations

Over the last decade, governments across the world have recognized the need to ensure online information and data privacy especially in relation to users' personal information on online social media and networking services. Although the privacy of sensitive personal information – such as health and medical records – has always been a priority, it is only recently that issues concerning the privacy of users' personal OSN information have gained prominence. This has partly been triggered by recent cases of privacy lapses on OSNs – such as the Facebook Beacon case – as well as by the development of privacy-invasive online social discovery applications – such as 'Girls Around Me' – and the recent controversy in Germany over Facebook's facial-recognition feature.

Historically, information and data privacy laws have differed greatly from one country to another. But in 1995, the European Parliament passed a law on information and data protection entitled *European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.[36] This directive required all EU member states to pass their own privacy laws based on the template offered by this directive. This also included the requirement to found a Data Protection Authority (DPA) to prevent and solve any issues related to data protection (Mayer-Schönberger, 1997). The 1995 EU Data Protection Directive thus provides a blueprint for current information and

[35] USA and Canada have been included owing not only to a large number of controversies in these countries concerning the online privacy of users but also because the different approaches taken by these countries help provide alternative views on online data use and privacy policies and regulations.

[36] EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. L 281

data privacy laws within various EU member states and lays down explicit guidelines concerning the following aspects:[37]

- Nature of the information gathered from users;
- Legitimacy of data processing;
- Categorizing different kinds of data processing;
- Providing users with the right to access the collected data;
- Providing users with the right to object to the processing of their information; and
- Ensuring the confidentiality and security of the gathered user information.

Nonetheless, the process of handling information and data privacy issues and concerns still varies greatly between European member states. A difference exists in the execution of the law and the power and resources of each DPA. This is caused by the incremental implementation of the directive upon preexisting national law. This implies that the same data protection transgression can be tried differently or more severely depending on the origin of the transgressor. Offenders are tried according to the law of the country they preside in, which means that, for example, a Belgian complaint about an English offending company cannot be followed by the Belgian law. The Belgian DPA (CBPL) communicates this to the English DPA (ICO), which then check whether the complaint is still applicable according to their law. However, most European countries enforce and implement some variant of information and data privacy laws based on the 1995 EU directive.[38] Table 2 provides an overview of the privacy laws/regulations/authorities within certain European nations as well as in USA and Canada.

Country	Law / Regulation / Authority
Austria	Data Protection Act (*Datenschutzgesetz*) of 2000
Belgium	Belgium Data Protection Law (1992) – modified later in 1998 to incorporate the Data Protecion Directive
Bulgaria	Personal Data Protection Act (2002)
Canada	Personal Information Protection and Electronic Data Act (PIPEDA, 2000) – as well as – via the Privacy Commissioner's office.
Czech Republic	Act on Protection of Personal Data (2000)
Denmark	Act on Processing of Personal Data (2000)
Finland	Finnish Personal Data Act (1999)
France	The National Commission on Informatics and Liberties (*Commission nationale de l'informatique et des libertés*) and the Data Protection

[37] Refer: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

[38] Refer to the section – *Extended Bibliography: Government and Industry Reports, Regulations, and Policies* – in this deliverable for links to detailed information about privacy laws, regulation, and policies.

	Directive in the French Data Protection Act of 1978
Germany	Federal Data Protection Act (*Bundesdatenschutzgesetz, 2001*) and Telecommunication Act (*Telekommunikationsgesetz*)
Greece	Law on the Protection of Individuals regarding the Processing of Personal Data (1997)
Hungary	Act of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interests – later superseded by the new Data Act (2012)
Iceland	Act 77 on the Protection of Privacy concerning the Processing of Personal Data (2001)
Ireland	Data Protection Act of 1998 (amendment in 2003)
Italy	Data Protection Code implemented in 2004 and Processing of Personal Data Act of 1997 (replaced the previous law on Protection of individuals and other subjects with regard to the processing of personal data of 1996)
Latvia	Law on Protection of Personal Data of Natural Persons (2000)
Netherlands	Dutch Personal Data Protection Act 2001 (*Wet bescherming persoonsgegevens*) and The Right to Privacy (Article 10 of the Dutch Constitution)
Norway	Act on Processing of Personal Data (2001)
Poland	Act on the Protection of Personal Data (1998)
Romania	Law 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data (2001)
Slovenia	Personal Data Protection Act (original 1999, amendments 2005 & 2007)
Sweden	Personal Data Protection Act 204/1998 (1998, full implementation 2001)
Switzerland	Swiss Federal Data Protection Act (1993, revised version in 2008)
United Kingdom	Freedom of Information Act, UK Data Protection Act of 1998, and Privacy and Electronic Communication (EC Directive) Regulations of 2003
United States	Industry-specific acts such as the Fair Credit Reporting Act and Electronic Communications Privacy Act (ECPA). A significant portion of information and data privacy laws are managed by the Federal Trade Commission (FTC) – an independent agency of the US government.

Table 2: Information Privacy Laws/Regulation/Authority by Country

On January 25, 2012, the European Commission laid down a proposal for a General European Data Protection Regulation (European Commission, 2012a). This regulation builds upon and strengthens existing privacy mechanisms across business practices, online networks, and

mobile applications. The regulations lay down data protection and privacy reforms in relation to upcoming technological innovations,[39] citizen rights concerning information privacy,[40] and the facilitation of international cooperation regarding the collection and processing of users' personal information.[41]

Specifically in relation to the privacy and security of users' personal information on social media services and OSNs, the Commission conducted a survey across European member states in which nearly two-thirds of the surveyed citizens indicated concerns over the fact that they feel they are giving away too much personal data online (European Commission, 2012b). In this regard, in addition to strongly advocating privacy by design, the commission has also proposed the 'privacy by default' option which dictates that the default sharing settings on social media and networking sites must be the ones that provide the maximum permissible level of user privacy. In terms of data transparency, the commission has also guaranteed users easier methods to access and edit their own data online (Ibid.).

An important and controversial strand concerning information privacy on online social media and networking technologies within this new regulation is the proposed *right to be forgotten and erasure* (Article 17). Article 17 provides individuals with the ability to selectively edit and erase already gathered, retained, transmitted, and processed personal information online. Box 2 provides an overview of the main features of Article 17 of the new European Data Protection Regulation of 2012; however, a few definitions are important to understand the jargon within the new directive (adapted from European Commission, 2012a):

- **Data subject:** Anyone whose personal information has been collected and/or processed.
- **Data controller:** Anyone who is responsible for and determines the purpose and means of the processing of the personal information collected.
- **Data processor:** Anyone who processes personal information of users' for a data controller.
- **Third-party:** Anyone who processes personal information of users' under the authority of a data controller or processor.

In the USA, as indicated in table 2, there is no single unified information and data privacy regulation. For example, the Health Insurance Portability and Accountability Act (HIPPA), the Fair and Accurate Credit Transactions ACT, and the Children's Online Privacy Protection Act (COPPA) deal only with specific issues in relation to the privacy and security of the personal information of a particular social group. Although the Supreme Court voted in favor of a constitutional right to privacy in the 1965 *Griswold vs. Connecticut* court case, very few American states have actually enforced this in practice. However, the state of California

[39] Refer: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf

[40] Refer: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

[41] Refer: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf

has enforced more comprehensive policy regulations concerning the online privacy of its residents – most notable being the 2003 California Online Privacy Protection Act (COPPA).

Particularly concerning the online privacy of young children, the COPPA enforces strict policies and regulations for the privacy protection of minors (children under the age of 13) on the Internet.[42] The law not only delimits the nature of personal information that companies can collect from minors but also directs these companies to ensure parental consent before legally collecting any personal information from minors. Owing to such strict rules, a large number of companies simply disallow minors from using their websites and services as it is much easier to simply ban children instead of dealing with the necessary requirement of first obtaining parental consent before gathering minors' personal information.

However, the FTC has recently updated COPPA to ensure greater privacy of minors' personal information (FTC, 2012a) and these rules will be effective from July 1, 2013. Whereas the older version of the Act was specifically targeted at websites catering only to minors, the FTC has now also included mobile apps, games, third-party plug-ins, and advertisement networks under the act. Moreover, in addition to photos and videos, the FTC has included geo-location data into the definition of personal information. In terms of liability exemptions, the FTC has indicated that a) it will not hold app stores liable for applications from other companies that attempt to gather information from minors, and b) it will allow for 'contextual advertising' to minors.[43]

In addition to government regulations and policies, there are also a number of independent institutes across Europe, USA, and Canada that handle information and data privacy issues and concerns. These include, for example, the European Network and Information Security Agency (ENISA) which works for EU member states and institutions to cater to cyber-security issues of the EU; FTC – independent agency working for the US government particularly in relation to consumer data and privacy protection; EU Kids Online Network – a multinational network coordinating empirical investigations into children's use of online services; Pew Research Center –an American non-governmental independent group working on informing people about general issues and trends that impact their lives; and industry research centers including those set up by Microsoft, Google, and Facebook.

[42] http://www.ftc.gov/ogc/coppa1.htm

[43] Prior to the FTC revision of COPPA, Facebook had requested the FTC in a filing to clarify that websites will still be permitted to display first-party advertising to minors in addition to tracking adult users of web services (Egan, 2012). Stressing the fact that the FTC has always differentiated between first- and third-party advertising, Facebook asked the FTC to ensure such a difference remains in the new act as well. The FTC approval for contextual advertising within the revised COPPA regulation thus seems to be in accordance with Facebook's request.

Box 2

Main Features: Article 17

(Adapted from European Commission, 2012a)

- **Data subject rights**

  The user has the rights to direct the data controller to erase the personal information that the controller has collected from the user. Moreover, the invoking of this right also implies that the controller can no longer disseminate this information to third parties.

- **Data controller obligations**

  Under the data subject rights, the data controller is obliged to take all reasonable technical and managerial steps to ensure that the user's demands are carried out. If the data controller transmitted the user information to third-parties, then the controller should also make sure to inform all of these parties to erase that particular piece of information as well as any links or reproductions of the data. Furthermore, if the controller has authorized any third party for publishing this user information, under Article 17 the controller shall take full responsibility for such a publication.

- **Data collection exceptions**

  Article 17 provides the following grounds on which the data controller is allowed to retain user information: a) in relation to the right to freedom of expression, b) concerning public interest in domain of public health, c) regarding research for scientific, statistical, and research purposes, and d) in case there is a legal obligation to retain the collected data.

- **Restricting rather than erasing**

  The article also provides special scenarios in which the controller is allowed to restrict the processing of personal information (rather than erasing it): a) during the time in which the accuracy of the data remains contested, b) the data is no longer being processed but is required for the purpose of proof, c) the processing being done is unlawful but the data subject does not want the data to be erased, and d) the data subject has requested the movement of his/her personal information from one data processing system to another.

Another important organization is the World Wide Web Consortium (W3C) – an Internet Standard Setting Organization. With regard to targeted advertising and how it relates to privacy issues there is the Digital Advertising Alliance (DAA), a coalition of media and marketing firms, which provides simplified choices to users to opt-in and out of targeted advertising online.

With regard to the differences in information and data privacy laws and regulations between Europe and USA, the EU and US Department of Commerce in 2000 made the 'safe-harbor' agreement which lays down procedures for American corporations to align themselves with the EU data privacy directives.[44] This helps American firms to operate with European users. Moreover, in wake of recent online privacy concerns the Obama administration has come up with a new framework for enforcing a revised version of the consumer data privacy and protection regulation. The Whitehouse Report directs the adoption of a Consumer Privacy Bill of Rights which provides more comprehensive guidelines for business organizations in relation to the collection, storage, transmission, and processing of consumers' online personal information. Box 3 provides an overview of the newly proposed Consumer Bill of Rights.

The four dominant features within information and data privacy policies, recommendations, and regulations across Europe and America are given below:

- **Privacy by Design**

  A strong focus within all policy recommendations and regulations is on the implementation of Fair Information Practices (FIPs) across technology development and management processes.[45] This is an attempt to embed preventive and proactive mechanisms within a technology's lifecycle to provide more robust means of information and data privacy and security. The strongest adherent of this principle is the office of the Canadian Privacy Commissioner. The Privacy Commissioner's official website provides a document outlining seven foundational principles for embedding privacy by design within technological development and management processes: 1) proactive approach, 2) default privacy settings, 3) embedding privacy into design, 4) accommodating majority of legitimate interests, 5) end-to-end security, 6) greater visibility and transparency, and 7) respect for user privacy.[46]

[44] http://export.gov/safeharbor/. These companies adopt the prescriptions defined in the safe-harbor agreement which offer an "adequate" level of data protection under Article 25 of the Directive.

[45] In the USA, the FTC has outlined a set of FIPs that organizations and third-parties have to comply with concerning the collection and processing of users' personal information. The FTC has drafted these FIPs around five core principles of privacy protection: 1) Notice/Awareness, 2) Choice/Consent, 3) Access/Participation, 4) Integrity/Security, and 5) Enforcement/Redress. For detailed information concerning these principle refer: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[46] Refer: http://privacybydesign.ca/about/principles

Box 3

A Consumer Privacy Bill of Rights

The 2012 Whitehouse Report on Consumer Data Protection lays down a Consumer Privacy Bill of Rights, indicating clear instructions for companies to provide more protection for consumers. The Bill of Rights clearly explicates a set of FIPs concerning the collection and processing of consumer information across industries and practices. Specifically, the bill addresses the following seven principles (The White House, 2012):

1. **Individual Control**

   A consumer has exclusive rights over the collection and processing of his/her personal information by companies.

2. **Transparency**

   A consumer has the right to easily comprehensible and accessible information about privacy practices and mechanisms of companies.

3. **Respect for Context**

   A consumer has the right to reasonably expect that companies will gather, transmit, and store his/her personal information in a manner that respects the context in which the consumer provided the information to the company.

4. **Security**

   A consumer has the right to secure and responsible handling of his/her personal information by companies.

5. **Access and Accuracy**

   A consumer has the right to access and edit the personal information collected and stored by companies in a manner that not only protects the sensitivity of the personal data but also reduces the risk of adverse consequences to consumers in case the data is inaccurate.

6. **Focused Collection**

   A consumer has the right to reasonable limits on the amount of his/her personal data that companies may collect, transmit, and store.

7. **Accountability**

   A consumer has the right to have his/her personal data processed by companies in a manner that complies with the Consumer Privacy Bill of Rights.

- **Increased Data Security within Data Collection, Retention, and Disposal processes**

  The need for greater data security within business practices is a primary objective across policy recommendations and reports. An explicit focus is on ensuring not only the security of the users' personal information that is collected and retained by business organizations and web services but also the responsible and privacy-preserving disposal of such information. Whereas the dominant focus concerning information security and privacy within industries is on strengthening the encryption and anonymity of stored personal information of users, it is also equally important to ensure the privacy-preserving nature of data disposal processes.

- **Increased Data Transparency and Access**

  In addition to increased data security, the majority of information and data privacy laws stress the need to provide more transparency to users not only concerning the nature of personal information that business organizations collect and process but also how and why these first-party organizations share their information with third-parties. A strong step in this direction is the provision of Data Download Tool (DDT) through which OSN and social media users can download a copy of their information that has been gathered and stored by particular online services and companies.

- **Understandable Privacy Policies and Simplified Consumer Choice**

  Governments across the world also agree upon the need to have more easily understandable privacy and data policies for consumers. Current privacy and data policy documents are not only quite long but also full of technical and legal jargon that a typical user finds difficult to understand. In addition to this, policy institutes also stress that simplified choices need to be provided to users concerning the security and privacy of their personal information online.

4.2 | Challenges: Multiplicity of concerns and issues

a) Privacy by design challenges

The importance of embedding privacy within the design and development phases of technologies and businesses in terms of FIPs has received considerable attention within a large number of governmental and non-governmental policy recommendations, regulations, and reports (Boyles, Smith, & Madden, 2012; European Commission, 2012a; FTC, 2012a, 2012b, 2012c, 2012d; Hobgen, 2007; Internet Safety Technical Task Force, 2008; The White House, 2012). Moreover, across Europe and USA, governments and research institutes have recognized the need to build privacy directly into the technology's development cycle by proactively anticipating privacy-invasive scenarios and embedding counter-measures into the technology beforehand. However, such policy approaches face a host of technical and managerial challenges concerning the logistics and feasibility of their implementation. With

regard to privacy by design policy recommendations and regulations, these challenges can be interpreted within five categories:

- Building privacy into existing technologies;
- Marginal uptake of alternate technologies;
- Ensuring necessary data collection while maintaining user privacy;
- Enforcing privacy mechanisms across services and countries; and
- Managing independent and unregulated technology development.

Building privacy into existing technologies

One of the biggest challenges facing information and data privacy policy-makers is the incorporation of privacy by design into already existing services and technologies. Since privacy by design approaches extend across all phases within the lifecycle of an application or technology, they have to be incorporated at a base level within each step of a technology's development and management lifecycle. Embedding such privacy mechanisms into already existing technologies is a difficult task. This difficulty is primarily based around the fact that incorporating privacy by design across services and applications requires a shift within existing business practices towards FIPs concerning data gathering, data transmission, and privacy disclosures.

Already existing technologies, such as Facebook and Google+, have a large user base in addition to a vast repository of user-generated content and communication. Since OSNs enable and facilitate large-scale communication, the content generated from such interactions becomes widely diffused across users, services, and applications. For a shift towards embedded privacy by design in such established services, FIPs need to be translated into standardized technical parameters such as engineering and usability practices for these to be implemented across applications and industries (Rubinstein & Good, 2012). This need for a translation of FIPs into codified engineering metrics and practices (and further enforcing of such standards) poses a substantial challenge to the enforcing of privacy by design across existing applications and industries that rely on and use already established data practices within and across technologies and businesses.

Box 4
Challenges to building privacy within existing technologies

To build privacy into already existing technologies, policymakers have to deal with multiple challenges such as:

- How to enforce and regulate privacy within the lifecycle of already developed and deployed services such as Facebook and Google+?
- In the wake of rapidly evolving nature of web applications, how can policy makers accurately predict and model privacy-invasive events beforehand?
- Simply recommending privacy by design is not enough anymore. It is more important to come up with a technical translation of FIPs into guidelines, metrics, and standardized parameters for these information practices to be enforceable within and across industries and applications.

Marginal uptake of alternate technologies

In line with privacy by design approaches and privacy-preserving policies, regulations, and mechanisms, a number of alternative online social media services and technologies have started to emerge. As discussed in section 2.2, these include for example distributed social networks such as Diaspora and buddycloud and privacy-enhancing technologies such as online proxies and cookie-tracking software. However, although such technologies allow users to have more control over their personal information, the uptake of such technologies is low in comparison to mainstream online services and applications. For example, Facebook remains the dominant choice for online social networking and has a user base of over a billion active members while 132 installations of Diaspora have just over 350,000 members (Diaspora Alpha, 2013).

Thus, the incorporation of privacy by design approaches and the development of privacy-preserving technologies is the first of many steps in resolving online privacy issues. A bigger challenge is to compel users to use these alternatives in place of mainstream applications and this task is increasingly becoming more and more difficult. This difficulty can be attributed primarily to two factors (adapted from Ingram, 2010):

- The use of alternate privacy-preserving technologies such as Diaspora requires users to have particular technical know-how and this plays a significant role in restricting the appeal of such technologies.
- Majority of users have already created detailed profiles and connections on existing social networks. Moreover, mainstream social networks are further connected to other

online social media technologies and often a user logs into other services using a standardized profile such as that of Facebook. Thus, at a time when users not only feel at ease with existing technologies but also have created connections and content across services – it becomes increasingly difficult to compel them to move towards other alternatives.

Ensuring sufficient data collection while maintaining user privacy

It is important to note that not all forms of data collection raise user privacy concerns. Certain forms of online data collection are in fact necessary to ensure the reliability and functionality of online services and applications. Companies gather a wide variety of information from their users ranging from technical data (e.g. browser type, operating system information, and IP address) to a user's personal data (e.g. name, email address, and zip code). Although this information is usually stored in an encrypted format to protect the users' privacy, the data itself can be associated with previously collected information of the same user to create a user profile. However, the degree to which such data collection leads to privacy issues depends primarily on how the collected information is used (FTC, 2012c).

For example, the use of such data to prevent online fraud and identity theft as well as to maintain user settings and choices across login sessions does not raise online information and data privacy concerns. On the other hand, uniquely identifiable information such as IP address and device IDs may in fact be used by application developers and certain network analytics companies to create detailed user profiles. Moreover, since uniquely identifiable information usually remains the same across applications and services, these user profiles may not be limited to one particular application but rather contain information collected from multiple sources. For example, a detailed user profile may contain a user's name, address, mobile number, zip code, Facebook friends' data, song preferences, previous online shopping details, web history, as well as location data.

The use of such detailed information, without the user's explicit consent, to target specific advertisements or to track the user's movement across web services raises a host of privacy concerns. Business practices (such as targeted advertising and market research) often take precedence over user privacy concerns. However, as discussed above, certain forms of data collection are in fact required and thus policy-makers face a unique challenge in terms of finding a balance between necessary minimal data collection and preventing the misuse of the gathered data in terms of user profiling.

Enforcing privacy mechanisms across services and countries

Online social media and networking technologies are no longer stand-alone services. Increasingly there has been large-scale collaboration not only between OSNs such as Twitter, Facebook, and Google+ but also across OSNs and other applications such as e-commerce sites, online music services, and third-party mobile apps. Within social media and networking platforms, data moves seamlessly between multiple applications – each with its own privacy

mechanisms, user settings, and data processing means. Furthermore, as shown earlier in section 3.1, Facebook and Microsoft profiles are increasingly being used as virtual passports to log into other online social media services. This movement of user profiles across web services and applications leads to the attribution of multiple sets of information to the same user profile in addition to the already existing fluid nature of user content.

This relational and fluid character of user profiles and personal information necessitates technical interoperability of privacy mechanisms and policies across multiple web services. It is not only essential to incorporate FIPs into the technology development and management phases of individual services but also important to provide for standardized mechanisms and regulations to ensure privacy-preserving mechanisms for the communication and processing of user information between different sets of online social media and networking technologies. This poses substantial challenges for information and data privacy policy-makers concerning the enforcing and regulation of privacy by design approaches. Whereas a major focus in policy reports and documents is on building privacy within each step of a technology's lifecycle, it is also important to note that privacy lapses often occur when data moves from one online service to another.

Moreover, information and data privacy laws differ vastly between and across countries and continents. Every country has different provisions for the security and privacy of online user information; however, data on the Internet is not bound by physical limitations and it continuously moves between online services across countries. Thus, there is a need for establishing and promoting more consistent and globally interoperable privacy approaches and mechanisms for protecting consumer data across countries (FTC, 2012b).

Managing independent and unregulated technology development

A major logistical hurdle in implementing privacy by design approaches is the management and regulation of independent and non-commercial application development and management processes. Whereas mainstream OSNs, registered companies, and mobile applications on authorized app stores can be regulated through standardized policies, it is far more difficult to enforce and regulate FIPs and privacy by design mechanisms within independent and unregulated application development processes. With more and more information now available on the Internet concerning web and mobile app development as well as the use of social media and networking APIs within and across online applications, it is becoming much easier for independent engineers and startups to develop novel forms of social media and networking technologies.

This is clearly evident within upcoming privacy-invasive social discovery platforms such as Badabing and Girls Around Me. Although these applications are unique in that they gained significant negative coverage and Girls Around Me was even taken down from the Apple Appstore, not all applications and services are available on authorized app stores and often applications may only be used within smaller non-commercial groups. This poses a big management issue for information and data privacy policy makers in ensuring FIPs and

privacy-preserving mechanisms across multiple uses and applications of online social media and networking services in non-commercial DIY environments.

b) Mobile devices and privacy challenges

With mobile devices becoming a norm within contemporary society, policy makers are now also focusing on ensuring and enforcing strong privacy measures within and across mobile devices and applications. As discussed in section 2.3, in addition to OSN and app information, mobile devices also contain users' personal information such as contacts, photos, messages, and location data. Various first- and third-party mobile applications gather, transmit, and profile user device as well as personal information, raising many information and data privacy issues and concerns. Moreover, mobile devices and applications (particularly mobile gaming apps) are increasingly being used by minors and teenagers. Thus in addition to regulating and enforcing privacy by design across web services, the widespread diffusion of mobile devices coupled with the rapidly evolving nature of mobile services and applications poses even more challenges for information and data privacy policy-makers. These challenges can broadly be classified within two categories:

- Ensuring privacy of child users of mobile devices; and
- Regulating information privacy across multiple mobile platforms.

Small children and small devices

A large section of the mobile marketplaces, such as Apple Appstore and Google Play, is dedicated to children's games. These gaming apps have been found to gather, transmit, and store various kinds of user information including, but not limited to, mobile device ID, phone number, and geographical location (FTC, 2012c). Moreover, the developers of these apps rarely disclose either the privacy practices within the app or the interactive sharing features within the app itself to the children and their parents (FTC, 2012d). Parents usually do not interact with these applications and most of the time children operate mobile device on their own. The low-level of parental involvement, in addition to the fact that mobile device and personal data is often transmitted from these apps, means that policy makers need to understand and regulate the complex data-gathering mechanisms and information sharing/disclosure features within such applications.

In a survey of 400 mobile gaming apps taken from Apple Appstore and Google Play store, the FTC found out that whereas nearly 60% of apps gathered or transmitted mobile device information, only 20% of the apps actually disclosed any information about privacy features and practices (FTC, 2012c). Moreover, almost 60% of the apps contained in-app advertising, while only 15% of the apps indicated the presence of this advertising prior to the downloading of the app (Ibid.). These large gaps between data collection/transmission and privacy disclosures raise quite a challenge for policy-makers wanting to enforce stricter privacy mechanisms and guidelines on kids' mobile app developers.

Multiple platforms and information privacy

Different mobile devices run on different operating platforms such as Apple's iOS, Android, BlackBerry OS, and Windows. Each of these operating systems not only allows varying levels of user choice and control concerning the privacy and sharing of personal information but also provides different levels of user device and data control to app developers through their APIs. Nonetheless, the social mobiles apps developed on these platforms run across devices and communicate and share information with social media services and OSNs. Furthermore, as discussed in the earlier section, not all mobile apps contain a comprehensive data privacy policy. In research done across 2,600 mobile applications, it was discovered that iOS applications continuously access more information on mobile devices in comparison with Android applications (Han, Yan, Gao, Zhou & Deng, 2013). An important reason for this is the difference in the ways in which different operating systems enable varying levels of control to app developers. Thus, these differences within mobile operating systems pose particular challenges to information and data privacy policy makers in relation to developing and enforcing mobile interoperable privacy regulations across multiple devices and platforms. An important step in this direction has been taken by the California Attorney General who has directed all mobile developers to conspicuously provide and post their app's privacy policies to users.

5. Conclusions

In this report we have dealt with a multiplicity of factors concerning the security and privacy of users' personal information online. These factors include technological issues, industry standards, online identity formation, visible/invisible audience, publicly available information and research, young people's use of social media and OSNs, as well as policy challenges concerning privacy by design, and mobile devices and platforms. In this section, we summarize the main conclusions in relation to design, behavior and conduct and policy, and identify future research possibilities concerning the technological, social, and policy challenges with regard to online user privacy.

Privacy and Design

Online services, particularly social media and OSNs, are increasingly gaining importance within the everyday lives of people all over the world. From minors to adults, a large number of people interact with these technologies over a prolonged period of time. Moreover, social media and networking platforms allow developers to create particular applications for these platforms. Such large-scale and continuous interactions of mass self-communication across online services and applications produce vast quantities of online data. Although such Big Data has great potential for market research and service innovation, at the same time it raises a host of privacy issues and concerns. These issues include user profiling, third-party data abuse, development of privacy-invasive social discovery mobile apps, potential privacy threats to minors, and the collapsing of public and private contexts while sharing information online – particularly on mobile devices.

Social media, OSNs, and related third-parties gather a vast amount of user data to ensure the proper functioning of their services, to provide personalized and contextual user services, and to target specific advertisements to particular users. Owing to the large-scale sharing of data between multiple online services and applications, these organizations can then create rich profiles of users' personal information across computing devices and online services. Although the intricacies of data collection, storage, processing, and deletion are explicated within the T&C and privacy policies of online services, as explained in section 2 these are often quite lengthy and ridden with technical and legal jargon. This makes them highly ineffective as a legitimate means to gather user consent. The fact that a user has to comply with them in full makes them even more intrusive and ineffective.

Moreover, data agreements between online and offline companies – such as the one between Facebook and Datalogix – raise further privacy concerns owing to the merging of online and offline data into granular user profiles. The fact that options for opting-out of such data collaborations are not even presented on parent sites such as that of Facebook makes it even more difficult for users not only to opt-out of tracking but also to be aware of such tracking mechanisms in the first place. Furthermore, user data is collected in multiple ways making it difficult to manage and regulate information flows online. Whereas some data collection means are quite explicit, tracking a user through invisible cookies, widgets, and beacons is definitely a concern for a majority of users and governments worldwide.

Although a number of PPETs have been developed to provide alternative services to online users, as explained in section 4.2.a, the uptake of PPETs such as DSNs is quite marginal and often these tools are not very user-friendly. The relationship between PPETs such as DSNs and mainstream online services such as Facebook is indeed quite complex. The fact that DSNs provide granular data security and privacy mechanisms through a large number of options also means that a majority of users face difficulty in interacting with and using such networks. One way of dealing with this challenge is to provide fewer and simpler privacy settings on DSNs thereby making them more user-friendly. However, doing so can significantly alter (and even reduce) the perceived effectiveness of such systems in terms of user data privacy controls.

Concerning mobile devices such as smartphones and tablets, we have explained how the combination of personal sensitive mobile information, OSN data, and geolocation tagging on such devices can raise significant user privacy issues and concerns. People carry such devices with them and use a host of first- and third-party mobile applications on a variety of platforms such as Apple's iOS and Google's Android. These apps allow a user not only to perform particular tasks but also to use his/her location data to access personalized and contextual services such as searching for a restaurant nearby. We have shown in section 2.3.a that the use of specific location-based services in conjunction with data from other OSNs, in the form of social discovery mobile apps, can lead to privacy-invasive applications of social media, OSN, and mobile data. When a user consents to sharing information on two separate online platforms, he/she does not explicitly consents to combination of these isolated pieces of information.

Thus, although a number of industry standards and technologies provide users with the means to monitor, regulate, and restrict the flow of their online personal information, a lot of work still needs to be done in order to address and minimize online user privacy issues and concerns. Further investigation into online data gathering, retention, and processing mechanisms as well as into potential uses of location-based data can provide further clarity regarding online user privacy. Box 5 lists future research possibilities in relation to the industry standards and technological challenges (privacy and design) concerning online user privacy.

Box 5

Privacy and Design: Future research questions

- What are the current technological means of collecting, storing, processing, and deleting users' online personal information? How can these be classified?
- How are cookies used across online services? What is the nature of users' personal information and online activity tracked and transmitted by cookies?
- What are the privacy implications of social and behavioral advertising on online social media and networking technologies?
- What are the existing data collaboration agreements between online services? What is the nature and content of data shared across services?
- How can privacy policies be presented to the user in more conspicuous and easily-readable forms without undermining their technological and legal essence?
- What steps need to be taken to increase the uptake of PPETs such as DSNs in comparison with mainstream applications and services?
- What are the potential privacy-invasive combinations of location-based services and social media and networking information? How can user privacy and security concerns be addressed?
- What are potential uses and abuses of Big Data?

Privacy and Behavior/Conduct

Online services and applications are used by a large number of users who belong to different age groups, ethnicities, religions, and countries. Increasingly minors and young adults are also using online social media and networking services. Each person interacts with and uses online services and applications differently. Whereas certain users use online social media and networking services in order to develop and maintain a particular online identity, others merely use them as tools for communicating with colleagues, friends and family online. The way users define and understand online communication and sharing conduct specifies the nature of online privacy issues and concerns especially in relation to the use of social media and networking technologies. The inability to accurately translate social, behavioral and privacy norms and conduct into technological options and features makes it increasingly difficult for online users to effectively manage and regulate online communication. Moreover, sometimes users themselves are unable to understand particular privacy options and

mechanisms, thereby raising privacy issues and concerns such as with the recent Facebook private message scare.

As also explained in section 3.1, a substantial problem on online social media and networking services is the difference between intended/unintended and visible/invisible audiences (Litt, 2012). Users sometimes share information that is targeted towards specific audiences only. However, the nature of the technological platform on which they share or the privacy settings they use sometimes makes the information available to unintended audiences as well. In another instance, users are often unaware that the information they are sharing online is visible to a vast majority of users. Moreover, the 'public' privacy setting on a post fails to effectively communicate the magnitude of the outreach that a single share can have online.

Another important privacy issue concerning users' online social behavior and conduct is the potential threat to minors and young adult users of online social media and networking services. As we have already explained in section 3.2, the belief that young users do not care about their own online privacy is incorrect. Research has shown that young users are as concerned about their online privacy as adult users. Nonetheless, it is true that young users often find it difficult to comprehend the online privacy policies and regulations (sometimes ignoring such policies altogether) and this makes them highly vulnerable to online privacy breaches. Paternalistic methods often work with regard to children's use of online services, but with the widespread diffusion of computing and mobile devices it is quite difficult to exhaustively monitor their online usage and communication, thereby exposing them to privacy and security risks.

Thus, the social behavior and conduct of online users defines the nature of privacy issues and concerns online. Privacy by context is an important step in this direction – one in which information flows within and across online services are defined and shaped by social contexts (see: Nissenbaum, 2010). However, the feasibility and effectiveness of such an approach (in contrast with privacy by design and FIPs) still needs to be ascertained. Box 6 provides a list of future research questions concerning online privacy issues and concerns in relation to users' online social behavior and conduct.

Box 6
Privacy and Behavior/Conduct: Future research questions

- What are the uses of online social media and networking services? What different related privacy issues and concerns do they raise?
- How do users perceive intended/unintended and visible/invisible audiences?
- How can we minimize the privacy paradox in terms of finding a balance between necessary privacy settings and effective management of data by users?
- What is the feasibility and effectiveness of the privacy by contextual integrity approach?
- How do minors and young adults use social media and networking services particularly on mobile devices?
- What means and mechanisms can be developed to enable the use of publicly available data for research purposes in ways that preserve the privacy of user information?

Privacy and Policy

The need to ensure online information and data privacy especially in relation to users' personal information on online social media and networking services now features prominently on government agendas across the world. With a significant portion of the world's population now online, government agencies have to audit and regulate industry standards, mechanisms, and technological tools that are used for collecting, storing, and processing online user information. Moreover, increasingly official information about individuals, including tax and medical records are moving into the digital sphere, in turn raising further concerns over the security of such sensitive information. To address these concerns, policy makers face a large number of technological and managerial challenges, ranging from the difficulty of incorporating privacy by design across web services and applications to managing independent/unregulated technology development processes.

Countries and regions deal with user privacy issues and concerns differently. EU member states follow a detailed and comprehensive data use and privacy policy, largely shaped by the 1995 EU Directive on the protection and movement of user data. On the other hand, the USA has a fragmented approach towards user privacy and a number of American acts (such as HIPPA and COPPA) deal with specific issues concerning the privacy and security of online information. However, data on the Internet is not bound by political boundaries and it moves seamlessly within and across national borders. This makes it even more difficult for policy makers to effectively regulate online information. In this regard, the safe-harbor agreement between the USA and EU enables online organizations to comply with

data use and privacy policies across the two continents. Nonetheless, the recent controversies concerning Facebook in Ireland and Germany as well as the large number of court cases against social media and networking organizations worldwide showcase how the current policies and laws are still far from being effective.

Specifically concerning the technological and managerial challenges to user privacy and security policy making, there is a definite gap between policy-making processes on the one hand and the subsequent implementation of policies on the other.[47] A clear example of this is the recently proposed Article 17 – *right to be forgotten and erasure* – of the 2012 European Data Protection Regulation draft. First, the article imposes undue obligations on the data controller concerning the erasure of online information. The data controller is obliged to delete the stored information as well as to take all reasonable steps to ensure the deletion of the information that was either transmitted to third-parties or linked and copied elsewhere. On the Internet, where data continuously moves across applications and where copying a piece of information is as simple as clicking a button, such data controller obligations seem impractical in terms of actual implementation. Second, the article explicates the steps that need to be taken by the data controller/processor and third-parties to erase the user information but does not indicate how this can be done technologically. As we have indicated earlier in section 4.2.a, one of the biggest challenges regarding user privacy and security policy making is the translation of these regulations and policies into standardized technological mechanisms. For example, on an OSN where one piece of information is simultaneously linked to multiple users, applications, and services, erasing a single piece of information while ensuring the proper functioning of related entities is definitely a major technological challenge.

Thus, although governments and organizations across the world are focusing more and more on issues of online user privacy, there are still a number of technological and managerial challenges that policy makers need to overcome to effectively address and manage user privacy issues and concerns. A substantial challenge in this regard is the translation of policies and regulations into globally interoperable technological standards. As explained in section 4.2.a, not all data collection raises privacy concerns and policy makers also need to find a balance between necessary data collection and enabling effective user privacy regulations. In this respect, there is a need to develop a minimal data collection standard which defines the bare minimum level of information that online social media and networking technologies as well as ecommerce services can collect from users. Box 7 lists future research possibilities in relation to the technological and managerial challenges concerning user privacy and security policy making.

[47] Apart from the technological challenges to the implementation of Article 17, there is also the legal debate of 'Freedom of Speech' which could come into conflict with the 'Right to be forgotten and erasure'. For an overview of this problem refer to Hoven (2012).

Box 7
Privacy and Policy: Future research questions

- How can 'privacy by design' be incorporated within the lifecycle of already developed and deployed services such as Facebook and Google+?
- In the wake of rapidly evolving nature of web applications, how can privacy-invasive events be predicted and modeled?
- What are the minimal data collection limits across web services and applications?
- What steps need to be taken to bridge the gap between policy making processes and their subsequent technological and managerial implementation? For example, what steps need to be taken to implement Article 17 on online social media and networking services?
- How can existing data use/privacy policies be made globally interoperable?
- What steps need to be taken to ensure the regulation and management of user privacy within independent/unregulated technology development processes?
- What are the differences between traditional online services and mobile devices and apps? What further steps are needed to ensure the development and enforcing of effective data use and privacy policies across mobile devices and applications?

Bibliography

Aberer, K., Narendula, R., & Papaioannou, T. G. (2012). A Decentralized Online Social Network with Efficient User-Driven Replication. SocialCom 2012, Amsterdam, 2012.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technology*, *4258*, 36–58.

Awad, N. F., & Krishman, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13–28.

Baden, R., Bender, A., Bhattacharjee, B., Spring, N., & Starin, D. (2009). "Persona: an online social network with user-defined privacy," in Proc. of the ACM SIGCOMM.

Bakker, A., Epema, D. H. J., Garbacki, P., Iosup, A., Pouwelse, J. A., Reinders, M., Sips, H. J.van Steen, M. R., Wang, J., & Yang, J. (2008). "Tribler: a social-based peer-to-peer system: Research articles," Concurr. Comput: Pract. Exper., vol. 20, no. 2, pp. 127–138.

Balkin, J. M. (2004). Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society. Yale. Retrieved from http://digitalcommons.law.yale.edu/fss_papers/240/

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9).

Borisov, N. & Lucas, M. M. (2008). "Flybynight: mitigating the privacy risks of social networking," in Proc. of the WPES.

boyd, d. (2008a). Facebook's privacy trainwreck: Exposure, invasion and social convergence. *Convergence*, *14*(1), 13–20.

boyd, d. (2008b). *Taken Out of Context: American Teen Sociality in Networked Publics*. University of California-Berkeley.

boyd, D., & Marwick, A. (2011). Social steganography: Privacy in networked publics. *International Communication Association,* Boston, MA.

Boyles, J. L., Smith, A., & Madden, M. (2012). *Mobile Privacy and Data Management*. Washington D.C. Retrieved from http://pewInternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf

Brandtzæg, P. B., Luders, M., & Skjetne, J. H. (2010). Too many Facebook "friends"? Content Sharing and sociability versus the need for privacy in social network sites.

Buchegger, S., Datta, A., Schioberg, D., & Vu, L. H. (2009). "Peerson: P2P social networking: early experiences and insights," in Proc. of the ACM EuroSys Workshop on Social Network Systems.

Buchegger, S., Datta, A., & Rzadca, K. (2010). "Replica placement in p2p storage: Complexity and game theoretic analyses," in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on June 2010, pp. 599 –609.

C´aceres, R., Cox, L. P., Shakimov, A., & Varshavsky, A. (2009). "Privacy, cost, and availability tradeoffs in decentralized osns," in Proc. of the WOSN.

Carey, R., & Burkell, J. (2009). A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society* (pp. 65–82). Toronto: Oxford University Press.

Cassell, J., & Cramer, M. (2007). High Tech or High Risk: Moral Panics about Girls Online. In T. McPherson (Ed.), *Digital Youth, Innovation, and the Unexpected* (pp. 53–75). Cambridge, MA: MIT Press.

Castells, M. (2009). *Communication power*. Oxford: Oxford University Press.

Cho, C. H., & as-, U.O.T.A.A.I.A. (2004). Why do people avoid advertising on the Internet?. *Journal of advertising, 33(4),* 89-97.

Consolvo, S., Smith, I., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location disclosure to social relations: why, when, & what people want to share. *Proceedings of CHI 2005, conference on human factors in computing systems* (pp. 82–90). ACM Press.

Curtis, A. (2011). The Brief History of Social Media. *Mass Communication Department, Univesity of North Carolina*. Retrieved November 25, 2012, from http://www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html

Cutillo, L. A., Molva, R., & Strufe, T. (2009). "Privacy preserving social networking through decentralization," in Proc. of the WONS.

Debatin, M., Lovejoy, J. P., & Horn, A. (2009). Facebook and online privacy: attitudes, behaviours, and unintended consequences. *Journal of Computer Mediated Communication*, *15*, 83–108.

De Wolf, R. (2013). *Who's my audience again? How users perceive and manage their audience on online social networks.* Paper presented at ICA, London (UK).

Diaspora Alpha. (2013). How many users are in the DIASPORA network? *Diaspora Alpha*. Retrieved January 2, 2013, from https://diasp.eu/stats.html

DiMicco, J. M., & Millen, D. R. (2007). Identity management: multiple represenations of self in facebook identity. *Proceedings of GROUP'07* (pp. 383–386). Florida: ACM Press.

Egan, E. M. (2012). Facebook: FTC Filing COPPA. *FTC Documents*. Retrieved January 1, 2013, from http://www.ftc.gov/os/comments/copparulereview2012/561789-00100-84302.pdf

Ellison, N., Steinfield, C., & Lampe, C. (2011). Connection Strategies: Social capital implications of Facebook-enabled communication practices. *New Media and Society, 13(6),* 873-892.

European Commission. (2012a). *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Brussels. Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Commission. (2012b). *How will the data protection reform affect social networks?* Brussels. Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

Facebook. (2012). Key Facts - Facebook. *Facebook Newsroom*. Retrieved November 13, 2012, from http://newsroom.fb.com/Key-Facts

Fogel, J., & Nehmad, E. (2008). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160.

Francis, P., Guha, S., & Tang, K. (2008). "Noyb: privacy in online social networks," in Proc. of the WOSP, Seattle, WA, USA.

FTC. (2012a). FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule. Retrieved January 2, 2013, from http://www.ftc.gov/opa/2012/12/coppa.shtm

FTC. (2012b). *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy-makers*.

FTC. (2012c). *Mobile Apps for Kids: Disclosures Still Not Making the Grade*. Retrieved from http://www.ftc.gov/opa/2012/12/kidsapp.shtm

FTC. (2012d). *Mobile Apps for Kids Report*. Retrieved from http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

Ganjali, Y., Saroiu, S., Tootoonchian, A., & Wolman, A. (2009). "Lockr: better privacy for social networks," in Proc. of the CoNEXT.

Graffi, K., Hartung, D., Kovacevic, A., Menges, B., Mukherjee, P., & Steinmetz, R. (2009). "Practical security in p2p-based social networks," in Proc. of the IEEE LCN, October 2009.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (pp. 71–80). New York: ACM Press.

Han, J., Yan, Q., Gao, D., Zhou, J., & Deng, R. (2013). Comparing Mobile Privacy Protection through Cross-Platform Applications. Retrieved January 7, 2013, from http://www.liaiqin.com/hanjin/papers/NDSS2013Han.pdf

Heyman, R., De Wolf, R., & Pierson, J. (2012). Not all privacy settings are created equal - evaluating social media privacy settings for personal and advertising purposes. Paper presented at Political Economy section for IAMCR Conference 'South-North Conversations', 15-19 July, 2012, Durban, South Africa.

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry. *Electronic Commerce Research and Applications*, *9*(1), 50–60.

Hobgen, G. (2007). *Security Issues and Recommendations for Online Social Networks*.

Hoofnagle, C., Jay, K., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? *Social Science Research Network*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

Hoven, M. May 2, 2012. Balancing Privacy and Speech in the Right to Be Forgotten. *Harvard Journal of Law & Technology*. Retrieved from http://jolt.law.harvard.edu/digest/privacy/balancing-privacy-and-speech-in-the-right-to-be-forgotten

Ingram, M. (2010). Should Facebook be Worried About Diaspora? *Gigaom*. Retrieved December 1, 2012, from http://gigaom.com/2010/06/05/should-facebook-be-worried-about-diaspora/

Internet Safety Technical Task Force. (2008). *Enhancing Child Safety and Online Technologies*.

King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is there an app for that? *Proceedings of the Seventh Symposium on Usable Privacy and Security (p.12)*. Retrieved from http://cups.cs.cmu.edu/soups/2011/proceedings/a12_King.pdf

Krasnova, H., Spiekermann, S., Koroleva, K., &Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25 (2),* 109-125.

Lampe, C., Ellison, N., & Steinfield, C. (2008). Changes in Use and Perception of Facebook. *In Proceedings of the 2008 Conference on Computer-Supported Cooperative Work*.

Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011). *We're in it together: interpersonal management of disclosure in social network services*. Paper presented at the annual conference on Human factors in computing systems. CHI, New York (USA).

Lewis, K., Kaufman, J., & Christakis, N. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, *14*(1), 79–100.

Liau, A. K., Khoo, A., & Ang, P. H. (2005). Factors influencing adolescents' engagement in risky Internet behavior. *CyberPsychology & Behaviour*, *8*(2), 513–520.

Litt, E. (2012). Knock, Knock. Who's There? The Imagined Audience. *Journal of Broadcasting & Electronic Media, 56(3),* 330-345.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011, November). Analyzing Facebook privacy settings: User expectations vs. reality. *In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 61-70). ACM.

Livingstone, S., Olafsson, K., & Staksrud, E. (2011). *Social Networking, Age and Privacy*. Retrieved from http://www.eukidsonline.net/

Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). *Social Networking, Age and Privacy*. London, England. Retrieved from http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf

Madden, M. (2012). *Privacy management on social media sites*. Washington D.C. Retrieved from http://www.pewInternet.org/~/media/Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf

Martin, K. (2012). Information technology and privacy: conceptual muddles or privacy vacuums? *Ethics and Information Technology*, *14*(4), 267–284.

Mayer-Schönberger, V. (1997). *Das Recht am Info-Highway*. Orac.

Meyer, D. November 7, 2012. *Google's Chrome finally embraces Do Not Track, but with a warning*. Retrieved from http://www.zdnet.com/googles-chrome-finally-embraces-do-not-track-but-with-a-warning-7000007022/

Moreno, M. A., Parks, M., & Richardson, L. P. (2007). What are adolescents showing the world about their health risk behaviours on MySpace? *MedGenMed*, *9*(9).

Morris, M. R., Teevan, J., & Panovich, K. A. (2010). Comparison of Information Seeking Using Search Engines and Social Networks. *Proceedings of ICWSM* (pp. 291–294).

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. California: Stanford University Press.

Patchin, J., & Hinduja, S. (2010). Trends in online social networking: adolescent use of MySpace over time. *New Media and Society*, *12*(2), 179–196. Retrieved from none

Radin, T. J. (2001). The privacy paradox: E-commerce and personal information on the Internet. *Business Professional Ethics Journal*, *20*, 145–170.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1).

Rubinstein, I., & Good, N. (2012). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkley Technology Law Journal*, *Forthcomin*. Retrieved from http://ssrn.com/abstract=2128146

Solove, D. J. (2007). "I"ve got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.

Staddon, J., Huffaker, D., Brown, L., & Sedley, A. (2012). Are privacy concerns a turn-off?: Engagement and privacy in social networks. *In Proceedings of SOUPS, ACM Press*, 1-13.

Staksrud, E., & Livingstone, S. (2009). Children and online risk. *Information, Communication & Society, 12(3),* 364-387.

Stecher, K., & Counts, S. (2008). Thin Slices of Online Profile Attributes. *ICWSM-2008*. Seattle.

Strater, K., & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, InteractiondVolume 1. BCS-HCI '08* (pp. 111–119). Swinton, UK: British Computer Society.

Stutzman, F., & Kramer-Duffield, J. (2010). Friends Only: Examining a Privacy-Enhancing Behavior in Facebook. *CHI 2010*. Atlanta, GA.

Stutzman, F., Vitak, J., Ellison, N., Gray, R., & Lampe, C. (2012). Privacy in interaction: Exploring disclosure and social capital in Facebook. *In Proceedings of the 6th annual International Conference on Weblogs and Social Media (ICWSM).*

The White House. (2012). *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Washington DC.

Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web*. Heidelberg: Springer Verlag.

Tufekci, Z. (2008). Can You See Me Now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*, 20–36.

Van den Berg, B., & Leenes, R. (2010). Audience Segregation in social network sites. *2010 IEEE Second Internaional Confrence on Social Computing* (pp. 1111–1116). IEEE Press.

Weinstein, L. February 29, 2012. *Stop the 'Do Not Track' Madness.* Retrieved from http://www.wired.com/business/2012/02/opinion-weinstein-donottrack/

West, A., Lewis, J., & Currie, P. (2009). Students' Facebook "friends": public and private spheres. *Journal of Youth Studies*, *12*(6), 615–627. Retrieved from none

Wouters, P., Hellsten, I., & Leydesdorff, L. (2004). Internet Time and the Reliability of Search Engines. *First Monday*, *9*(10). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1177/1097

Wyatt, S. (2012). Ethics of e-research in humanities and social sciences. In D. Heider & A. Massanari (Eds.), *Digital Ethics* (pp. 5–20). New York: Peter Lang.

Yao, M. Z., Rice, E. R., & Wallis, K. (2007). Predicting User Concerns about Online Privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722.

Young, A. L., & Quan-Hasse, A. (2009). Information revelation and Internet privacy concerns on social network sites: a case study of Facebook. *C&T '09 Proceedings of the fourth international conference on communities and technologies*.

Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. *Ethics and Information Technology*, *12*, 313–325.

Appendices

Appendices A to I are the abstracts of the presentations in the Workshop on Internet, Trust, Reputation, Identity, and Privacy (TRIP 2012) organized by JRA5 on December 4, 2012, at the École Polytechnique Fédérale de Lausanne, Switzerland. The presentations can be found here: http://Internet-science.eu/trip-workshop-dec-2012/presentations

Appendix A

'Slide to Unlock?' – Mobile convergence and collapsing contexts

Samir Passi (Royal Netherlands Academy of Arts and Sciences, KNAW)

This presentation will highlight privacy issues raised by increasing access to social networks made possible by various mobile applications. I will focus on the unintended consequences of the ability of third-party apps to interact not only with the online databases and services of social networks but also with a user's personal data within the mobile device itself. The content of the presentation is based on the review work that I am currently doing for the EINS JRA 5.1.1 deliverable (Analysis of Privacy, Reputation, and Trust in Social Networks) and relates to the disciplines of Science and Technology Studies (STS) and Information and Communication Technology (ICT).

Online social networks – which primarily started out as web services – have now evolved into social platforms that not only serve individual users but also offer developers the means to interact with the platform. Social networks such as Facebook, Foursquare, and Google+ provide programming interfaces that developers can use to build applications that can interface and interact with the platform's data and services. Depending upon the nature of the network, these third-party applications can then generate novel means to catalogue, classify, and correlate information pertaining to the entire user base of multiple social platforms. A famous example is the TweetDeck application that allows its users to simultaneously interact with Facebook and Twitter.

With the widespread diffusion of smartphones and tablets, such ability for novel and large-scale convergence of social information has implications for the sociology of user expectations concerning user information privacy. Through their mobile variants, these applications can scan a user's contacts, messages, mobile photos, and location in addition to information from various social platforms. This sometimes leads to situations where the ability of these apps to 'use' the gathered data has unintended consequences. An oft-cited example of this was 'Girls around me'. Through this app, a person could search around his/her location for nearby girls. The app took public data from Foursquare and coupled it with the public images of girls on Facebook to provide the user with an interactive map displaying a comprehensive visualization of information pertaining to girls around his/her location. Although the app was subsequently taken down, the example clearly depicts how third-party social applications can have consequences for societal notions of privacy and trust

by facilitating novel means of large-scale tagging, identifying, and converging not only online information but also the exact locations of mobile users.

An in-depth understanding of public and private contexts in relation to characteristics particular to the mobile medium provides a relevant point of entry to examine such privacy and trust issues. Although Facebook photos and Foursquare check-ins might have separately been made public by certain users, the combination of the two coupled with an exact location on the map is certainly not what these girls explicitly consented to. By identifying and merging particular bits of scattered information, apps such as 'Girls around me' facilitate the collapsing of public and private contexts and pose a substantial threat not only to an individual's privacy and personal security but also to socially acceptable forms of data mining.

Moreover, although such apps can be regulated on standardized app-stores provided by Google or Apple, the ease of working with social and mobile platforms makes it increasingly difficult to manage and govern the intentionality of the large number of mobile apps that are developed each day. Social networks and mobile devices have now become ubiquitous tools that are used by individuals to manage their everyday lives and mobile app development has become a substantial market in itself. In such a scenario, it is imperative to examine the implications of the ability of third-party applications to facilitate the large scale convergence of user information in ways that are quite novel and non-traditional. In a time when 'privacy as contextual integrity' and 'privacy by design' are issues that are featured prominently on the societal agenda, this presentation will provide insights into questions such as what contextual integrity translates to for the increasingly ubiquitous mobile medium or what we must know before we start designing privacy into mobile apps and social platforms?

Appendix B

PEDE: A Cloud-Based Personal Execution and Data Hosting Environment

Rayman Preet Singh, S. Keshav and Tim Brecht (University of Waterloo)

Increasing amounts of data are being generated and collected by, on behalf of, and about individuals. Some of this data is generated by traditional applications and services like document processors, e-mail, media-sharing services, web browsers, instant messaging, and social networking services. Other emerging sources of data include devices that act as sensors to record data such as smart metering, heath-care monitoring, smartphone-based sensing, and monitoring of individuals' banking and shopping activities. Most often, data is collected by service providers who take ownership and full control of the data – thereby risking users privacy - in exchange for free services. There is a growing discomfort among consumers about relying on the service providers' changing privacy policies, losing data privacy and control, and having to trust these services. This is evident from dissent against leading social networking and media sharing services, and cases of serious user resistance to the installation of smart meters collecting energy consumption data. These concerns are not without warrant as recent research has demonstrated that such data can be mined to reveal private information about users. For instance, energy consumption data from smart meters can be used to determine occupancy, appliance use, and even the TV channel being watched! Other forms of user data such as messaging, photos, videos, location, health statistics, spending activities are unarguably private in nature and their collection by service providers poses new threats to user privacy. However, keeping user data completely private makes it impossible to make data driven recommendations to users that could benefit them. Our goal is to build an environment that balances data privacy and data analytics.

We propose constructing a framework in which users place their data at a universally accessible location that they own and control individually. A user's data resides in the cloud within her Personal Execution and Data Environment (PEDE) which provides reliable storage for hosting the data, and computation to run applications on the data. The use of modern clouds for hosting PEDEs relieves the user of the problems of warehousing the data, its accessibility, computation resources for its processing, and its consolidation from multiple sources, which arise when commodity devices are used for the purpose. Users download applications to their PEDEs and they interface with users' data and other services a PEDE may offer. Being a PEDE owner, a user can configure applications' access to the data (and services) and can impose her own privacy policies, enabling a privacy-preserving application ecosystem for the data, which remains under her purview at all times. In this ecosystem, third party developers build applications that process the data, generating meaningful results for the user, enhancing data value, while fully respecting users' data ownership, privacy and control. Much like app stores for mobile devices that have enriched the user experience, such an ecosystem would enable innovation in data processing which is currently frozen because of user data being locked with service providers.

We are studying a cloud-based architecture that uses PEDEs to allow users to provide third parties with fast, consolidated, universal, and privacy-preserving access to their data while retaining complete ownership and control of the data. We build example applications to demonstrate how appliance vendors, energy auditors, and other third parties can develop consumer applications using our platform while preserving consumer privacy. Possible use cases of this platform include: applications performing detailed analysis, tailored to individual users, for quantifying benefits of purchasing energy efficient appliances, and for helping users better understand and control their energy consumption.

Prior work has recognized the problem of data privacy and offered theoretical advances, such as differential privacy and homomorphic encryption. It provides protocols that protect the privacy of the data while enabling computations on that data. Unfortunately, prior work does not describe systems to enable application development and deployment. Our work is unique in that it leverages the rich infrastructure of modern clouds to provide an environment for the implementation of these algorithms.

Appendix C

Protecting the Privacy of Personal Data through Change of Ownership

Yves-Alexandre de Montjoye, Alex “Sandy” Pentland (MIT Media Lab)

Personal data—digital information about users' location, web-searches, and preferences—is undoubtedly the oil of the new economy. However, the same smart algorithms which conveniently advise you on the next movie you should watch or restaurant you should eat at can also infer more than you might want to from seemingly harmless data.

Our contribution is two-fold. First, we argue that as soon as personal data becomes rich enough, it cannot be generically anonymized without severely limiting its uses. Second, we introduce openPDS, a privacy-preserving personal data store. openPDS allows for generic, on-the-fly uses of personal data while protecting user privacy. Such a user-centric model defines a new paradigm for protecting Internet privacy.

In this work, we review existing privacy literature and de-anonymization methods with a focus on high-dimensional data and, more particularly, on location data. We argue that there are no privacy preserving methods that anonymize the data a priori for a broad range of uses. Such limitations make it essential for users to control their personal data. A change of data ownership has thus been proposed by the National Strategy for Trust Identities in Cyberspace, The Department of Commerce Green Paper, the Office of the President’s International Strategy for Cyberspace, and the European Commission's 2012 reform of the data protection rules.

We introduce openPDS, an implementation of this new ownership model through a personal data store owned and controlled by the user. openPDS supports the creation of smart, data-driven applications while protecting the privacy of users’ personal data. As openPDS allows for third-party applications to be installed, sensitive data processing can take place within a user's PDS through a secure question answering framework. This framework allows the dimensionality of the data to be reduced on a per-need basis before being anonymously shared. Unlike existing methods, such a privacy-preserving scheme does not require access to the whole database. openPDS also engages in privacy-preserving group computation to aggregate data across users. This framework simplifies a lot of the traditional security problems such as broad query restrictions and abuses, security of cloud storage, or reputation and trust systems. Our initial deployment monitored through smartphones the daily behavior of a set of individuals with diagnosed mental problems and offered a first qualitative evaluation of the system. A large-scale deployment will start in Trento Italy in November in partnership with Telecom Italia.

As technologists and scientists, we are convinced that there is an amazing potential in the use of personal data, but also that benefits should be balanced with risks. By reducing the dimensionality of the data on the fly or by anonymously just answering questions, openPDS opens up a new way for individuals to regain control over their privacy, while allowing them to unlock the full value of their data.

Appendix D

Online Reputation Management: A perspective from the industry

Dr. Laura Toogood (Digitalis Reputation, London)

The field of Online Reputation Management (ORM) has emerged as an increasingly important component of the digital industry. Over the last couple of years, a select number of specialist firms have been successfully operating in this sector. Through the emergence of a professional field of ORM, it is clear that there is a recognised need for private individuals, corporate organisations and products to manage their online reputation.

The online reputation needs of private clients typically include dealing with crisis situations, general online profile management and constant monitoring of the Internet to help mitigate risk. Individuals typically become frustrated when the search profile for their name is considered an unfair representation or contains negative content. Another key concern is the longevity of third party generated content, which ranks highly for the client name. Such content can consist of archives of newspapers or other commentary that is available to users of search engines. This content is considered to have a more permanent impact on a client's reputation than the print equivalent.

Private clients that engage with ORM are principally apprehensive about the lack of ability to control their profile in the online space. A common requirement relates to securing a presence on the SERPs, in order to ensure that Internet users view authentic and controlled content as a result of a search query.

Some of the processes of ORM include overseeing individual projects, devising strategy and deploying resources, in order to address such client concerns. Various technical strategies enable the manipulation of search engine results pages (SERPs) in order to ensure a client has the desired online profile when Internet users search for certain keywords. Content that is perceived as positive or neutral by the individual is typically promoted to rank highly in the SERPs, thus demoting negative content.

Some individuals do not want an obvious Internet presence and require some level of anonymity to be implemented. Others desire a strong presence and require advice on utilising personal websites and social media profiles. Client's requiring the latter commonly demonstrate a lack of skill and understanding about using web assets and are nervous about how to portray their persona online.

Therefore, ORM not only addresses the SERPs, but also encompasses social media use, as well as online branding and positioning. Collaborative work takes place between ORM experts, reputation lawyers, publicists, private security firms and PR companies to service the needs of private clients.

ORM is an area of research that fits into the use of social media content as a resource in personal strategies of manipulation and maintenance of online persona. Therefore, the demand for ORM poses some important questions: What causes certain individuals to place value on how they are portrayed in the online space? Is it possible for your physical reputation to be

aligned with an online persona and can these become unified and communicated successfully in the digital space?

From an industry viewpoint, I will present some case studies that have been anonymised, along with a number of suggestions for future research. This will illustrate the need for developing a clearer understanding of what drives certain individuals to engage with ORM.

Appendix E
How to build, measure & use 'social reputation' to foster better democracy

Marco Bani (Scuola Superiore Sant'Anna)

For several years governments invested significant resources in the digital management of democratic processes. Furthermore, e-government, with the introduction of ever more collaborative and immersive digital tools, such as social media, has moved away from the simple digitalization of document processes, organizational and decision-making within the administration, towards a new model that involves citizens (and communities of) in the co production and sharing of information, provision of services and participatory policies, which may lead to a new reconsideration of e-democracy theories.

These processes require the acquisition and management of a large amount of information, which rise some questions about the profiles related to the protection of individuals and social control. It is not just a matter of privacy, but the new online interactions promoted by social media require a greater mutual accountability and a better evaluation of others social aspects such as reputation, trust and acknowledgements.

Trust in institutions has been steadily declining in the Western democracies and the possibility of developing a real partnership between citizens depends on the degree of transparency and accountability they are able to offer. Governments should be more reachable, available and relevant to users, delivering responsiveness of policy to technological change and fostering a "call to action" of their citizens, giving motivations that will encourage usage of government services through online platforms. Motivations which do not necessarily being financially, but mainly related to "social reputation", the true currency of web.

The value of reputation is not a new concept to the online world: we can see that whether in e-commerce sites, as the star ratings on Amazon or the PowerSellers system on eBay, or in online communities, from the smallest one to the biggest, such as Wikipedia. People understand that the way they behave online will impact their ability to maintain a presence on those sites as well as perform all sorts of transactions in the future. In the same way citizens who help their local community would be recognized for the vital role they play in generating different kinds of wealth for society. "Social currency" enables people to connect and collaborate like never before and shape public sphere where innovations occur and anyone can benefit from the adoption of new technologies and ideas. Moreover, in the development of civic actions, a very high degree of trust is required between strangers, and democratic stakeholders (governments, citizens and civil society) need to conceive "social currency" as an accurate and legitimately powerful tool and encourage users not to misuse it, to make digital and social identities actually truly reflect participation in democratic process, acknowledging participation according to fair and equality principles.

A reliable system of "social reputation" is needed to avoid the high risk of pollution of participatory policies by corporations, lobbyists or people who want to affect negatively for their own good, already present in great numbers in the actual digital public sphere. Besides that, the methods and resources used so far for trust in peer policies are fundamentally

disorganized. In the past year, a plethora of reputation services have launched to serve as the connective tissue of reputation and trust across the web. But no one has risen as standard for use in e-government process. The various reputation systems differ not only in their approaches and implementation, but also in guiding principles. This uncertainty prompts a number of key questions: Is it possible to rank trustworthiness in the digital public sphere for e-democracy processes? Is it possible to use tools and principles already used in web communities to calculate "social reputation"? Is user data from social media useful in increasing trust? Will a single "social reputation" score work across multiple platforms? And what procedures are in place to ensure users' privacy, the accuracy of the rankings, the ability to address mistakes in rankings and the necessary acknowledgments to reward who is actively involved in civic engagement?

This paper analyzes innovative practices in the evaluation of "social reputation" to support the participation of citizens (and communities) in a reshaped public sphere, and recommends principles in order to foster a more active and trustful engagement, guessing that having an accountable social reputation system holds enormous potential for sectors where trust is fractured, such as politics and actual democracy.

Appendix F

Specifying Trust in Virtual Organizations

Jacques Calmet (Karlsruhe Institute of Technology, KIT)

Will the interplay between virtual and real worlds leads to an interdisciplinary modeling of nature suitable to information society? The obvious prototype would be an Internet of Things. There are several features to assess before answering this question. A first one is that the most successful approaches to interdisciplinary visions of many fields of human knowledge have relied on well-identified domains of mathematics. Among them one may cite algebra, geometry and analysis first, then logic and statistics and now topology. The second feature is that we aim at a knowledge society. An obvious reason to promote interdisciplinary approaches is to enable progresses. A first question is whether sociology has an impact on our answer. The answer is obviously positive.

There are several concepts that play a part in this game. A first one is trust. A knowledge society cannot exist without an abstract model of trust. It is not enough to build trust on beliefs. We must refine what we mean by trust. A second one is that the ultimate goal is to reach and make decisions based upon the available knowledge once the trust requirement is fulfilled. We may also interpret this has proving theorem/decisions in a cognitive world. We set our approach within models of multi-agent systems. Such a methodology is adopted in most fields derived from distributed artificial intelligence including business. This implies to deal with a society of agents.

From a computer science point of view we need to specify what we compute. Because Gödel and Turing have precisely defined what computability means, we must extend the concept of specification along epistemological purposes. We propose an algebraic specification inspired by methodologies and techniques designed and implemented for the mechanization of mathematics. This talk will outline some of them.

One must also assess the goals for designing the architecture of a relevant system. For instance, a design concept is to enforce a bottom-up approach. Another one is to assume, although the methodology is based on non-trivial mathematics, that users are not expected to have a background in this domain. Some examples are given to illustrate the kind of challenges set to this approach.

Appendix G

An Exploratory Study on how Customers feel Towards the EU Cookie Law, and if it affects their Trust towards a Website

Ninia Azzopardi (Oxford Brookes University)

Past research on Internet privacy has observed how consumers are concerned about the privacy of their online information and how easy it is for companies to gather, store and share this information. As e-consumers are lacking the knowledge on cookies, this research focuses on whether the change in the Privacy and Electronic Communications (Amendment) Regulations 2011 law (The Cookie Law) will affect e-consumers' trust towards a website, as websites must now require consent from users and provide information about the purpose of storing cookies.

Based on past research, it was found that the following six variables; Perceived Privacy, Perceived Security, Perceived Risk, Context, Quality and Consumers' Propensity to Trust, affect online trust.

The research approach adopted in this dissertation was a qualitative exploratory study which was carried out through fifteen interviews. All respondents were asked about how they feel towards the six variables before and after the law was implemented, and their views towards the Cookie Law.

The results showed that users perceived the Cookie Law to be positive and a step in the right direction, though they feel that companies fail to ensure compliance with the law. Surprisingly, the findings also showed that most users seem to be unaware of the existence of this law, even though it was enforced to help users control their data.

The main conclusions drawn from this study is that users' trust is unlikely to change as they believe that if they do not trust the website they will unlikely trust the cookie policy, though if there is third party accreditation then users' trust will decrease when using the website. Furthermore, as users are now more aware of the law and its purpose, 56% of the respondents said that in the future they will look out for it.

Appendix H
Identity and Trust: The Foundations of Privacy

Karmen Guevara (University of Cambridge)

Historically, the notion of privacy has evolved in response to technology. New layers of privacy have evolved in response to concerns over the intrusion introduced by new technologies. This creates a powerful dynamic between the social technologies and the inherent need for privacy and restrictions on disclosure which underlie human behaviors. Such motivations contribute to privacy becoming a far more complex construct, due to the underlying socio-cultural and psychological factors.

Identity and trust are fundamental to privacy. Maintenance of privacy is held to be conserved through trust. Therefore, our focus is on identity. So trust is considered within this context. An examination of identity is based on the axes around which the formation of identity occurs and its dimensions are at the root of the continuous construction process of building an identity. The dynamic tensions that lie at the core of identity are considered with the implications for in real life and on-line trust and privacy behaviors.

The new dimensions of identity that are emerging from the interactions with social technologies are giving rise to new trust heuristics and privacy behaviors. These are explored in juxtaposition with the chasm that exists between users in real life and on-line privacy behaviors during this period in which a new layer of privacy is being evolved.

Trust, privacy and disclosure behaviours are drawn from subconscious emotional drives and responses. Therefore, the examination of identity and privacy is framed around the subconscious processes underlying behaviours. The theoretical framework applied is drawn from Psycognition which is based on the theory that behavioral motives originate from the subconscious and therefore are significant because they directly influence individuals' perceptions and conscious behaviors.

A Psycognitive perspective is different from a purely psychological one, in that it takes a holistic socio-cultural systemic perspective of behaviours and the underlying subconscious processes**.** The Psycognitive approach is drawn from the disciplines of Human Sciences, Integral Theory, Evolutionary Psychology and Holistic Psychotherapy.

The methodology explored here includes the models applied in such an examination, for example, the *Organisation of Experience*, the *Dynamic Feedback Loop* and a *Psycognitive Layered Architecture*. Conclusions are drawn from the data collected from an aggregation of field studies in which investigations of individuals' core beliefs and behaviours relating to trust, privacy and security were conducted.

Appendix I
Competitive Value of Data Protection: The Impact of Data Protection Regulation on Online Behavior

Prof. Alessandro Mantelero (Politecnico di Torino)

In many contexts and debates, data protection laws are considered as an undue burden over enterprise activities, limiting their business opportunities, reducing their innovation in offering customized services and increasing their operating costs.

Some studies have demonstrated the limits and the lack of empirical evidence of these assumptions. On the one hand, the costs related to data protection are low and in many cases have indirect positive effects on different aspects, especially in terms of increased level of enterprise data security. On the other hand, although some projects find a barrier in data protection rules, in many cases this is due to an inadequate design of the project, focused on technical or business profiles without taking into adequate consideration the aspects concerning the protection of individuals.

At the same time, the increasing demand of individuals to have their privacy respected has generated new privacy-oriented services, increasing competition and innovation. From this perspective, the individual and social attitude towards privacy assumes a significant role in business activities and could become an important element in order to build trust in service providers. On the other hand, the lack of data protection increases the risks of illegitimate access to information or misuse of personal data, with a potential chilling effect on individual propensity for sharing and communicating personal information.

These needs become more relevant and perceived in the context of social networks, where service providers are collecting large amount of data (Big Data) in order to extract predictive information about individuals and social groups. In this sense, the recent EU proposal for a general data protection regulation contains different elements that can reinforce trust in data management. We could identify three different main lines in the proposal that have positive effects on trust in data management: reinforcement of attention to the design of the data processing, increased compliance to legal data protection framework, reinforcement of user's rights.

Historically, data protection rules attach great importance to the technological aspects concerning the processing of information, in order to define adequate procedure that guarantee a high level of protection. In this sense the data protection impact assessment, the privacy by design/by default approach and the preference for minimizing data collection are different solutions suitable to increase user's trust in the management of their data. At the same time, data portability and a more detailed regulation on the right to be forgotten reinforce the self-determination of the user in the social networks. Finally, the uniform approach adopted by the regulation, the different remedies and solutions adopted in order to increase the compliance to data protection rules (sanctions, audit, data breach notification, labelling) constitute further elements suitable to reinforce user's confidence.

Having made this initial assessment of the new EU Proposal for a general data protection regulation, it is important to define and analyse the role of identity management systems in social networks and their impact on profiling. From this perspective, the interaction between government and private sector in the field of authentication systems, the prevention of the risks of social control and the importance to preserve anonymity with regard to the freedom of expression assume particular relevance. An uncertain framework on these different aspects can have a negative impact on users, limiting freedom, self-determination and interaction in social networks.

Extended Bibliography

The following sections contain a list of scholarly, government, and industry publications (categorized according to type) concerning the issues of privacy, reputation, trust, and identity on online social networks and services.

Journal Articles

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technology*, *4258*, 36–58.

Acquisti, A., & Gross, R. (2009). Predicting Social Security Numbers from Public Data. *Proceedings of the National Academy of Sciences*, *106*(27), 10975–10980.

Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. *First Monday*, *13*(3).

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk and governance. *Surveillance & Society*, *2*(4), 479–497.

Awad, N. F., & Krishman, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13–28.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9).

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*, *2*(1), 46–55.

boyd, d. (2007). Social Network Sites: Public, Private, or What? *The Knowledge Tree*, *13*.

boyd, d. (2008). Facebook's privacy trainwreck: Exposure, invasion and social convergence. *Convergence*, *14*(1), 13–20.

boyd, d. (2011). Dear voyeur, meet Flâneur… Sincerely, Social Media. *Surveillance & Society*, *8*(4), 505–507.

boyd, d., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1). Retrieved from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Brandtzæg, P. B., Luders, M., & Skjetne, J. H. (2010). Too many Facebook "friends"? Content Sharing and sociability versus the need for privacy in social network sites. *International Journal of Human Computer Interaction*, *26*, 1006–1030.

Burgoon, J. K., Parrott, R., & Le Poire, B. A. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social & Personal Relations*, *6*, 131–158.

Calo, M. (2010). People can be so fake: a new dimension to privacy and technology. *Pennsylvania State Law Review*, *9*(114).

Christopherson, K. M. (2006). The positive and negative implications of anonymity in Internet social interactions: On the Internet, nobody knows you're a dog. *Computers in Human Behavior*, *23*(6), 3038–3056. Retrieved from none

Citron, D. (2010). Fulfilling Government 2.0's Promise with Robust Privacy Protections. *George Washington Law Review*, *78*(4), 822–845.

Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy Marketing*, *19*(1), 20–26.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Ellison, N., Lampe, C., & Steinfield, C. (2009). Social Network Sites and Society: Current Trends and Future Possibilities. *Interactions Magazine*, *16*(1).

Ellison, N., Steinfield, C., & Lampe, C. (2006). The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, *12*(3). Retrieved from http://jcmc.indiana.edu/vol12/issue4/ellison.html

Fahey, T. (1995). Privacy and the Family. *Sociology*, *29*(4), 687–703.

Fogel, J., & Nehmad, E. (2008). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. Retrieved from none

Fuchs, C. (2011). An alternative view of privacy on Facebook. *Information*, *2*, 140–165.

Fuster, G. G. (2010). Inaccuracy as a privacy-enhancing tool. *Ethics and Information Technology*, *12*, 87–95.

Gatt, A. (2002). Click-wrap agreements: the enforcability of click-wrap agreements. *Computer Law & Security Report*, *18*(6), 404–410.

Gelman, L. (2009). Privacy, free speech, and "blurry-edged" social networks. *Boston College Law Review*, *50*, 1315–1344.

Goodings L., L. A., & Brown, S. D. (2007). Social networking technology: place and identity in mediated communities. *Journal of Community & Applied Social Psychology*, *17*(6), 463–476. Retrieved from none

Green, N., & Smith, S. (2004). "A Spy in your Pocket"? The Regulation of Mobile Data in the UK. *Surveillance & Society*, *1*(4), 573–587.

Gregg, M. (2008). Testing the Friendship: Feminism and the limits of online social networks. *Feminist Media Studies*, *8*(2), 206–209. Retrieved from none

Grimmelmann, J. (2009). Facebook and the social dynamics of privacy. *Iowa Law Review*, *95*(4).

Gross, E. F. (2004). Adolescent Internet Use: What we expect, what teens report. *Journal of Applied Developmental Psychology*, *25*(6), 633–649.

Hargittai, E. (2007). Whose Space? Differences Among Users and Non-Users of Social Network Sites. *Journal of Computer-Mediated Communication*, *13*(1).

Hashemi, Y. (2009). Facebook's privacy policy and its third-party partnerships: Lucrativity and liability. *Boston University Journal of Science and Technology Law*, *15*, 140–161.

Hermans, L., Vergeer, M., & D'Haenens, L. (2009). Internet in the Daily Life of Journalists: Explaining the use of the Internet by Work-Related Characteristics and Professional Opinions. *Journal of Computer-Mediated Communication*, *15*(1), 138–157.

Hinduja, S., & Patching, J. (2008). Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace. *Journal of Adolescence*, *31*(1), 125–146.

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry. *Electronic Commerce Research and Applications*, *9*(1), 50–60.

Hodge, M. J. (2006). The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com. *Southern Illinois University Law Journal*, *31*, 95–122.

Hodkinson, P. (2007). Interactive Online Journals and Individualisation. *New Media and Society*, *9*(4), 625–650.

Hodkinson, P., & Lincoln, S. (2008). Online Journals as Virtual Bedrooms? Young People, Identity and Personal Space. *YOUNG*, *16*(1), 27–46.

Hoofnagle, C., Jay, K., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? *Social Science Research Network*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

Hope, A. (2007). Risk Taking, Boundary Performance and Intentional School Internet "Misuse". *Discourse*, *28*(1), 87–99.

Hui, K., Teo, H., & Sang-Yong, T. L. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19–33.

Hull, C., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: privacy issues on Facebook. *Ethics and Information Technology*, *13*, 289–302.

Humphreys, L. (2007). Mobile Social Networks and Social Practice: A Case Study of Dodgeball. *Journal of Computer-Mediated Communication*, *13*(1).

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100.

Jernigan, C., & Behram Mistree, F. T. (2009). Gaydar: Facebook friendships expose sexual orientation. *First Monday*, *14*(10).

Jones, H., & Soltren, H. (2005). Facebook: Threats to Privacy. *Social Science Research*, *1*, 1–76.

Jones, S., Millermaier, S., Goya-Martinez, M., & Schuler, J. (2008). Whose Space is MySpace? A content analysis of MySpace profiles. *First Monday*, *13*(9).

Kerr, I. (2001). The Legal Relationship Between Online Service Providers and Users. *Canadian Business Law Journal*, *35*, 1–40.

Kerr, M. H. S. (2000). What parents know, how they know it, and several forms of adolescent adjustment: Further support for a reinterpretation of monitoring. *Developmental Psychology*, *36*(3), 366–380.

Kramer, N., & Winter, S. (2008). Impression Management 2.0: The Relationship of Self-Esteem, Extraversion, Self-Efficacy, and Self-Presentation Within Social Networking Sites. *Journal of Media Psychology: Theories, Methods, and Applications*, *20*(3), 106–116. Retrieved from none

Lampe, C., Ellison, N., & Steinfield, C. (2008). Changes in Use and Perception of Facebook. *In Proceedings of the 2008 Conference on Computer-Supported Cooperative Work*.

Lange, P. (2007). Publicly Private and Privately Public: Social Networking on YouTube. *Journal of Computer-Mediated Communication*, *13*(1).

Le Blond, S., Zhang, C., Legout, A., Ross, K., & Dabbous, W. (2011). I know where you are and what you are sharing. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference - IMC '11* (p. 45). New York, New York, USA: ACM Press. doi:10.1145/2068816.2068822

Lewis, K., Kaufman, J., & Christakis, N. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, *14*(1), 79–100.

Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A., & and Christakis, N. (2008). Tastes, ties, and time: A new social network dataset using Facebook.com. *Social Networks*, *30*(4), 330–342. Retrieved from none

Liau, A. K., Khoo, A., & Ang, P. H. (2005). Factors influencing adolescents' engagement in risky Internet behavior. *CyberPsychology & Behaviour*, *8*(2), 513–520.

Liu, H., Maes, P., & Davenport, G. (2006). Unraveling the taste fabric of social networks. *International Journal on Semantic Web and Information Systems*, *2*(1), 42–71.

Livingstone, S. (1998). Mediated childhoods: A comparative approach to young people's changing media environment in Europe. *European Journal of Communication*, *13*(4), 435–456.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*, 393–411.

Livingstone, S., & Helsper, E. J. (2007). Taking risks when communicating on the Internet: the role of offline social-psychological factors in young people's vulnerability to online risks. *Information, Communication & Society*, *10*(5), 619–644.

Lugano, G. (2008). Mobile social networking in theory and practice. *First Monday*, *13*(11).

Mack, D., Head, A., Roberts, B., & and Rimland, E. (2007). Reaching Students with Facebook: Data and Best Practices. *Electronic Journal of Academic and Special Librarianship*, *8*(2).

Martin, K. (2012). Information technology and privacy: conceptual muddles or privacy vacuums? *Ethics and Information Technology*, *14*(4), 267–284.

Marwick, A. (2008). To Catch a Predator? The MySpace Moral Panic. *First Monday*, *13*(6).

Mayer, A., & Puller, S. L. (2008). The old boy (and girl) network: Social network formation on university campuses. *Journal of Public Economics*, *92*(1-2), 329–347.

Mazer, J. P., Murphy, R. E., & Simonds, C. J. (2007). I'll See You On "Facebook": The Effects of Computer-Mediated Teacher Self-Disclosure on Student Motivation, Affective Learning, and Classroom Climate. *Communication Education*, *56*(1), 1–17.

Michelfelder, D. P. (2001). The moral value of informational privacy in cyberspace. *Ethics and Information Technology*, *3*, 129–135.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, *27*, 27–32.

Moreno, M A, Parks, M. R., Zimmerman, F. J., Brito, T. E., & Christakis, D. A. (2009). Display of Health Risk Behaviors on MySpace by Adolescents: Prevalence and Associations. *Archives of Pediatrics Adolescent Medicine*, *163*(1), 27–34. Retrieved from none

Moreno, M A, VanderStoep, A., Parks, M. R., Zimmerman, F. J., Kurth, A., & Christakis, D. A. (2009). Reducing At-Risk Adolescents' Display of Risk Behavior on a Social Networking Web Site: A Randomized Controlled Pilot Intervention Trial. *Archives of Pediatrics Adolescent Medicine*, *163*(1), 35–41. Retrieved from none

Moreno, M.A., Parks, M., & Richardson, L. P. (2007). What are adolescents showing the world about their health risk behaviours on MySpace? *MedGenMed*, *9*(9).

Muise, A., Christofides, E., & Desmarais, S. (2009). More Information than You Ever Wanted: Does Facebook Bring Out the Green-Eyed Monster of Jealousy? *CyberPsychology & Behavior*, *12*(2), 441–444. Retrieved from none

Nissenbaum, H. (1997). Towards an approach to privacy in public: Challenges of Information Technology. *Ethics & Behaviour*, *7*, 201–219.

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, *17*, 559–596.

Papacharissi, Z. (2009). The Virtual Geographies of Social Networks: A comparative analysis of Facebook, LinkedIn and ASmallWorld. *New Media & Society*, *11*, 199–220. Retrieved from none

Park, N., Kee, K. F., & Valenzuela, S. (2009). Being immersed in social networking environment: Facebook Groups, uses and gratifications, and social outcomes. *CyberPsychology & Behavior*, *12*(6), 729–733. Retrieved from none

Patchin, J., & Hinduja, S. (2010). Trends in online social networking: adolescent use of MySpace over time. *New Media and Society*, *12*(2), 179–196. Retrieved from none

Pearson, E. (2009). All the World Wide Web's a stage: The performance of identity in online social networks. *First Monday*, *14*(3).

Raacke, J., & Bonds-Raacke, J. (2008). MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking sites. *Cyberpsychology & Behavior*, *11*(2), 169–174. Retrieved from none

Radin, T. J. (2001). The privacy paradox: E-commerce and personal information on the Internet. *Business Professional Ethics Journal*, *20*, 145–170.

Rau, P. P., Gao, Q., & and Ding, Y. (2008). Relationship between the level of intimacy and lurking in online social network services. *Computers in Human Behavior*, *24*(6), 2757–2770. Retrieved from none

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1).

Rubinstein, I., & Good, N. (2012). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkley Technology Law Journal*, *Forthcoming*. Retrieved from http://ssrn.com/abstract=2128146

Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., & Rao, J. (2009). Understanding and capturing people's privacy policies in a mobile social networking application. *Persuasive Ubiquitous Computing*, *13*, 401–412.

Sessions, L. (2009). "You looked better on MySpace" Deception and authenticity on Web 2.0. *First Monday*, *14*(7). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2539/2242

Sheldon, P. (2008). The Relationship Between Unwillingness-to-Communicate and Students Facebook Use. *Journal of Media Psychology: Theories, Methods, and Applications*, *20*(2), 67–75. Retrieved from none

Shoemaker, D. W. (2010). Self-exposure and exposure of the self: informational privacy and the presentation of identity. *Ethics and Information Technology*, *12*, 3–15.

Skog, D. (2005). Social interaction in virtual communities: The significance of technology. *International Journal of Web Based Communities*, *1*(4), 464–474.

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Solove, D. J. (2007). "I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.

Srivatsa, M., & Hicks, M. (2012). Deanonymizing mobility traces. *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12* (p. 628). New York, New York, USA: ACM Press. doi:10.1145/2382196.2382262

Sveningsson Elm, M. (2009). "Teenagers get undressed on the Internet" - Young people's exposure of bodies in a Swedish Internet community. *Nordicom Review*, *30*(2), 87–103.

Thiel, S., Bourimi, M., Giménez, R., Scerri, S., Schuller, A., Valla, M., Wrobel, S., et al. (2012). A Requirements-Driven Approach Towards Decentralized Social Networks. In V. Leung, C. Wang, T. Shon, & J. Park (Eds.), *Future Information Technology, Application, and Service: Lecture Notes in Electrical Engineering Vol. 164* (pp. 709–718). Netherlands: Springer.

Trottier, D. (2011). Mutual Transparency or Mundane Transgressions? Institutional Creeping on Facebook. *Surveillance & Society*, *9*(1/2), 17–30.

Tufekci, Z. (2008). Can You See Me Now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*, 20–36.

Tufekci, Zeynep. (2008a). Can You See Me Now? Audience and Disclosure Management in Online Social Network Sites. *Bulletin of Science and Technology Studies*, *11*(4), 544–564.

Tufekci, Zeynep. (2008b). Grooming, Gossip, Facebook and Myspace: What Can We Learn About These Sites From Those Who Won't Assimilate? *Information, Communication, and Society*, *11*(4), 544–564.

Tynes, B. M. (2007). Internet Safety Gone Wild?: Sacrificing the Educational and Psychosocial Benefits of Online Social Environments. *Journal of Adolescent Research*, *22*(6), 575–584. Retrieved from none

Utz, Sonia. (2010). Show me your friends and I will tell you what type of person you are: How one's profile, number of friends, and type of friends influence impression formation on social network sites. *Journal of Computer Mediated Communication*, *15*(2), 314–335. Retrieved from http://www3.interscience.wiley.com/cgi-bin/fulltext/123248036/HTMLSTART

Utz, Sonja, & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2).

Valkenburg, P M, & Peter, J. (2008). Adolescents' Identity Experiments on the Internet: Consequences for Social Competence and Self-Concept Unity. *Communication Research*, *35*(2), 208–231. Retrieved from none

Valkenburg, Patti M, Peter, J., & Schouten, A. P. (2006). Friend Networking Sites and Their Relationship to Adolescents' Well-Being and Social Self-Esteem. *Cyberpsychology & Behavior*, *9*(5), 584–590. Retrieved from none

Van Doorn, N. (2009). The Ties That Bind: The Networked Performance of Gender, Sexuality, and Friendship on MySpace. *New Media and Society*, *12*(4), 583–602. Retrieved from none

Watts, D. J., Dodds, P. S., & Newman, M. E. J. (2002). Identity and Search in Social Networks. *Science*, *296*, 1302–1305.

West, A., Lewis, J., & Currie, P. (2009). Students' Facebook "friends": public and private spheres. *Journal of Youth Studies*, *12*(6), 615–627. Retrieved from none

Wyatt, S. (2012). Ethics of e-research in humanities and social sciences. In D. Heider & A. Massanari (Eds.), *Digital Ethics* (pp. 5–20). New York: Peter Lang.

Yao, M. Z., Rice, E. R., & Wallis, K. (2007). Predicting User Concerns about Online Privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722.

Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. *Ethics and Information Technology*, *12*, 313–325.

Books and Conference Proceedings

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In P. Golle & G. Danezis (Eds.), *Proceedings of the 6th Workshop on Privacy Enhancing Technologies* (pp. 36–58). Cambridge: U.K. Robinson College.

Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era*. Lawrence: University Press of Kansas.

Backstrom, L., Dwork, C., & Kleinberg, J. (2007). Wherefore art thou r3579x? Anonymized social networks, hidden patterns, and structural steganography. *Proceedings of the 16th international conference on World Wide Web* (pp. 181–190).

Barkhuus, L. (2004). Privacy in location-based services, concern vs. coolness. *Proceedings of workshop paper in mobile HCI 2004 workshop: location system privacy and control*. Glasgow, UK.

Barocas, S., & Nissenbaum, H. (2009). On Notice: The Trouble with Notice and Consent. *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*. Cambridge, MA.

Blasbalg, J., Cooney, R., & Fulton, S. (2012). Defining and Exposing Privacy Issues with Social Media. In J. Meinke (Ed.), *Papers of the Twenty-first Annual CCSC Rocky*

Mountain Conference (pp. 6–14). Denver: The Journal of Computing Sciences in Colleges.

Bolter, J. D., & Grusin, R. (1999). *Remediation: Understanding New Media*. Cambridge, Mass.: MIT Press.

Boneva, B., Quinn, A., Kraut, R., Kiesler, S., & Shklovski, I. (2006). Teenage Communication in the Instant Messaging Era. In R. Kraut, M. Brynin, & S. Kiesler (Eds.), *Computers, Phones and the Internet: Domesticating Information Technology* (pp. 201–218). Oxford, New York: Oxford University Press.

Bonneau, J., Anderson, J., & Danezis, G. (2009). Prying Data Out of a Social Network. *Proceedings of the 2009 International Conference on Advances in Social Network Analysis and Mining* (pp. 249–254). Washington D.C.: IEEE Computer Society.

boyd, D. (2004). Friendster and Publicly Articulated Social Networks. *Proceedings of ACM Conference on Human Factors in Computing Systems (CHI 2004)* (pp. 1279–1282). ACM Press.

boyd, d. (2006a). G/localization: When Global Information and Local Interaction Collide. *O'Reilly Emerging Technology Conference*. San Diego, CA.

boyd, d. (2006b). Identity Production in a Networked Culture: Why Youth Heart MySpace. *AAAS 2006*. St. Louis, Missouri.

boyd, d. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *MacArthur founding series on digital learning - youth, identity and digital media volume* (pp. 119–142). MA: MIT Press.

boyd, d. (2008). *Taken Out of Context: American Teen Sociality in Networked Publics*. University of California-Berkeley.

boyd, D., & Heer, J. (2006). Profiles as Conversation: Networked Identity Performance on Friendster. *Proceedings of Thirty-Ninth Hawai'i International Conference on System Sciences (HICSS-39), Persistent Conversation Track*. IEEE Press. Retrieved from http://www.danah.org/papers/HICSS2006.pdf

Brake, D. (2009). Shaping the "Me" in MySpace: The Framing of Profiles on a Social Network Site in Digital Storytelling, Mediatized Stories: Self-Representations in New Media. In K. Lundby (Ed.), *Digital Storytelling, Mediatized Stories: Self-representation in New Media* (pp. 285–300). New York: Peter Lang. Retrieved from none

Canny, J., & Duan, T. (2004). Protecting user data in ubiquitous computing environments: towards trustworthy environments. *Proceedings of privacy-enhancing technologies (PET)*. Toronto.

Carey, R., & Burkell, J. (2009). A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society* (pp. 65–82). Toronto: Oxford University Press.

Cassell, J., & Cramer, M. (2007). High Tech or High Risk: Moral Panics about Girls Online. In T. McPherson (Ed.), *Digital Youth, Innovation, and the Unexpected* (pp. 53–75). Cambridge, MA: MIT Press.

Chew, M., Balfanz, D., & Laurie, B. (2008). (Under)mining Privacy in Social Networks. *Web 2.0 Security and Privacy*. Retrieved from http://w2spconf.com/2008/papers/s3p2.pdf

Clark, L. S. (2005). The Constant Contact Generation: Exploring Teen Friendship Networks Online. In S. Mazzarella (Ed.), *Girl Wide Web* (pp. 203–222). New York: Peter Lang Publishing.

Cocking, D. (2008). Plural selves and relational identity. In J. van den Hoven & J. Weckert (Eds.), *Information Technology and moral philosophy* (pp. 123–141). Cambridge: Cambridge University Press.

Coenen, T., Kenis, D., Damme, C. V., & Matthys, E. (2006). Knowledge Sharing over Social Networking Systems: Architecture, Usage Patterns and Their Application. *OTM Workshops* (pp. 189–198). Retrieved from none

Consolvo, S., Smith, I., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location disclosure to social relations: why, when, & what people want to share. *Proceedings of CHI 2005, conference on human factors in computing systems* (pp. 82–90). ACM Press.

DiMicco, J. M., & Millen, D. R. (2007). Identity management: multiple representations of self in Facebook identity. *Proceedings of GROUP'07* (pp. 383–386). Florida: ACM Press.

Driscoll, C., & Gregg, M. (2008). Broadcast Yourself: Youth, Community and Intimacy Online. *Youth, Media and Culture in the Asia-Pacific Region* (pp. 71–86). Cambridge Scholars Press. Retrieved from none

Dwyer, C. (2007). Digital Relationships in the "MySpace" generation: Results from a Qualitative Study. *Proceedings of the Fortieth Hawaii International Conference on System Sciences*. Los Alamitos, CA: IEEE Press.

Dwyer, C., & Hiltz, S. R. (2008). Designing privacy into online communities. *Proceedings of Internet Research 9.0*.

Erikson, E. H. (1980). *Identity and the Life Cycle*. New York: W.H. Norton and Co.

Ermecke, R., Mayrhofer, P., & Wagner, S. (2009). Agents of Diffusion - Insights from a Survey of Facebook Users. *Proceedings of the Forty-second Hawaii International Conference on System Sciences (HICSS-2007)*. IEEE Press. Retrieved from none

Felt, A., & Evans, D. (2008). Privacy protection for social networking APIs. *Proceedings of Web 2.0 Security and Privacy*. Oakland.

Felt, Adrienne, Hooimeijer, P., Evans, D., & Weimer, W. (2008). Talking to Strangers Without Taking Their Candy: Isolating Proxied Content. *SocialNets '08: Proceedings of the 1st Workshop on Social Network Systems*, 25–30. Retrieved from http://www.cs.virginia.edu/felt/secure_mashups.pdf

Fono, D., & Raynes-Goldie, K. (2006). Hyperfriends and Beyond: Friendship and Social Norms on LiveJournal. In M. Consalvo & C. Haythornthwaite (Eds.), *Internet Research Annual Volume 4: Selected Papers from the AOIR Conference* (pp. 91–103). New York: Peter Lang.

Girard, A., & Fallery, B. (2009). E-recruitment: new practices, new issues. An exploratory study. *3rd International Workshop on Human Resource Information Systems (HRIS 2009), in conjunction with ICEIS 2009*. Milan, Italy.

Gjoka, M., Sirivianos, M., Markopoulou, A., & Yang, X. (2008). Poking Facebook: Characterization of OSN Applications. *Proceedings of the first workshop on Online social networks*.

Golder, S., Wilkinson, D., & Huberman, B. (2007). Rhythms of Social Interaction: Messaging within a Massive Online Network. *Proceedings of Third International Conference on Communities and Technologies* (pp. 41–66). Springer.

Gosling S. D., G. S., & Vazire, S. (2007). Personality Impressions Based on Facebook Profiles. *Proceedings of ICWSM 2007*. Retrieved from none

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (pp. 71–80). New York: ACM Press.

Guha, S., Tang, K., & Francis, P. (2008). NOYB: Privacy in Online Social Networks. *Proceedings of the first workshop on Online social networks*.

Heer, J., & boyd, D. (2005). Vizster: Visualizing Online Social Networks. *IEEE Proceedings of Symposium on Information Visualization (InfoVis 2005)* (pp. 33–40). IEEE Press.

Jenkins, H. (2006). *Convergence Culture: Where old and new media collide*. New York: New York University Press.

Kapoor, N., Konstan, J., & Terveen, L. (2005). How Peer Photos Influence Member Participation in Online Communities. *Proceedings of ACM CHI 2005*.

Kerr, I. (Ed.). (2008). *Lessons from the Identity Trail*. Oxford: Oxford University Press.

Krishnamurthy, B., & Wills, C. E. (2008). Characterizing Privacy in Online Social Networks. *Proceedings of the first workshop on Online social networks*.

Lai, L. S. L. (2007). Impacts of Web 2.0 Based Social Networks; The Good, The Bad and The Ugly. *Conference on Information Management and Internet Research*. Edith Cowan University, Joondalup, Western Australia. Retrieved from none

Lai, L. S. L. (2008). So Far Away, Yet So Near: Social Connectedness of Travellers on Social Networking Sites. *IADIS International Conference e-Commerce*. NH Grand Hotel Krasnapolsky, Amsterdam, the Netherlands. Retrieved from none

Lampe, C., Ellison, N., & Steinfeld, C. (2006). A face(book) in the crowd: social searching vs social browsing. *Proceedings of CSCW-2006* (pp. 167–170). ACM Press.

Lampe, C., Ellison, N., & Steinfeld, C. (2007). A Familiar Face(book): Profile Elements as Signals in an Online Social Network. *Proceedings of Conference on Human Factors in Computing Systems (CHI 2007)* (pp. 435–444). ACM Press.

Lampe, C., Ellison, N., & Steinfield, C. (2008). Changes in Use and Perception of Facebook. *In Proceedings of the 2008 Conference on Computer-Supported Cooperative Work*.

Larsen, M. C. (2007). Understanding Social Networking: On Young People's Construction and Co-construction of Identity Online. *Internet Research 8.0: Let's Play*. Vancouver.

Lederer, S., Mankoff, J., & Dey, A. K. (2003). Who wants to know what when? Privacy preference determinants in ubiquitous computing. *Proceedings of extended abstracts of CHI 2003* (pp. 724–725). Fort Lauderdale, FL: ACM Press.

Lee, A. Y., & Bruckman, A. S. (2007). Judging you by the company you keep: dating on social networking sites. *In Proceedings of the 2007 international ACM conference on Supporting group work* (pp. 371–378). Retrieved from none

Li, C., & Bernhoff, J. (2008). *Groundswell: Winning in a World Transformed by Social Technologies*. Massachusetts: Harvard Business Press.

Liben-Nowell, D., Novak, J., Kumar, R., Raghavan, P., & Tomkins, A. (2005). Geographic routing in social networks. *Proceedings of National Academy of Sciences* (Vol. 102 (33), pp. 11623–11628).

Lipford, H. R., Hull, G., Latulipe, C., Besmer, A., & Watson, J. (2009). Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. *Proceedings of the Workshop on Security and Privacy in Online Social Networking, IEEE International Conference on Social Computing (SocialCom)*.

Livingstone, S. (2002). *Young People and New Media: Childhood and the Changing Media Environment*. London: Sage.

Livingstone, S. (2006). Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family. In R. Kraut, M. Brynin, & S. Kiesler (Eds.), *Computers, Phones and the Internet: Domesticating Information Technology* (pp. 128–144). Oxford, New York: Oxford University Press.

Livingstone, S. (2007). Internet Literacy: Young People's Negotiation of New Online Opportunities. In T. McPherson (Ed.), *Digital Youth, Innovation, and the Unexpected* (pp. 101–122). Cambridge, MA: MIT Press. Retrieved from none

Martínez Alemán, A. M., & Wartman, K. L. (2009). *Online Social Networking on Campus: Understanding what matters in student culture*. New York: Routledge.

Marwick, A. (2005). "I'm a Lot More Interesting than a Friendster Profile': Identity Presentation, Authenticity and Power in Social Networking Services. *AOIR 6.0*. Chicago, IL.

Masso, P. (2006). A Survey of Trust Use and Modeling in Current Real Systems. *Trust in E-services: Technologies, Practices and Challenges*. Idea Group.

Matthews, S. (2008). Identity and Information Technology. In J. Weckert (Ed.), *Information technology and moral philosophy* (pp. 142–160). Cambridge: Cambridge University Press.

Morris, M. R., Teevan, J., & Panovich, K. A. (2010a). Comparison of Information Seeking Using Search Engines and Social Networks. *Proceedings of ICWSM* (pp. 291–294).

Morris, M. R., Teevan, J., & Panovich, K. A. (2010b). What Do People Ask Their Social Networks, and Why? A Survey Study of Status Message Q&A Behavior. *Proceedings of CHI2010* (pp. 1739–1748).

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. California: Stanford University Press.

Nurullah, A. S. (2007). The Sociology of Cyberspace: Youth Online Networking and Cyberfriendship Formation. *8th Conference of the Asia Pacific Sociological Association*. Penang, Malaysia. Retrieved from none

Onnela, J. P., Saramaki, J., Hyvonen, J., Szabo, G., Lazer, D., Kaski, K., Kertesz, J., et al. (2007). Structure and tie strengths in mobile communication networks. *Proceedings of the National Academy of Sciences* (Vol. 104(18), pp. 7332–7336). Retrieved from none

Paolillo, J. C., & Wright, E. (2005). Social network analysis on the semantic web: Techniques and challenges for visualizing foaf. In V. Geroimenko & C. Chen (Eds.), *Visualizing the Semantic Web: XML-based Internet and Information Visualization* (pp. 229–242). London: Springer Verlag. Retrieved from http://www.blogninja.com/vsw-draft-paolillo-wright-foaf.pdf

Patil, S., & Lai, J. (2005). Who gets to know what when: configuring privacy permissions in an awareness application. *Proceedings of the SIGCHI conference on human factors in computing systems (CHI 2005)* (pp. 101–110).

Peter, J., & Valkenburg, P. M. (2011). Adolescents' online privacy: toward a developmental perspective. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web* (pp. 221–234). Heidelberg: Springer Verlag.

Pike, J. V, Bateman, P. J., & Butler, B. S. (2009). I Didn't Know You Could See That: The Effect of Social Networking Environment Characteristics on Publicness and Self-Disclosure. *Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California August 6th-9th 2009*.

Ploderer, B., Howard, S., & Thomas, P. (2008). Being online, living offline: The influence of social ties over the appropriation of social network sites. *Proceedings of CSCW 2008*.

Ploderer, B., Howard, S., Thomas, P., & Reitberger, W. (2008). "Hey world, take a look at me!": Appreciating the human body on social network sites. *Proceedings of Persuasive 2008* (pp. 245–248).

Preibusch, S., Hoser, B., Gürses, S., & Berendt, B. (2007). Ubiquitous social networks ? opportunities and challenges for privacy-aware user modelling. *Proceedings of the Workshop on Data Mining for User Modelling at UM 2007*.

Senft, T. (2008). *Camgirls: Celebrity and Community in the Age of Social Networks*. New York: Peter Lang.

Siibak, A. (2007). Casanovas of the Virtual World. How Boys Present Themselves on Dating Websites. *Young People at the Crossroads: 5th International Conference on Youth*

Research (pp. 83–91). Petrozavodsk, Republic of Karelia, Russian Federation. Retrieved from none

Solove, D. J. (2007). *The future of reputation: Gossip, rumour and privacy on the Internet*. New Haven: Yale University Press.

Spertus, E., Sahami, M., & Buyukkokten, O. (2005). Evaluating similarity measures: a large-scale study in the Orkut social network. *Proceedings of 11th International Conference on Knowledge Discovery in Data Mining (KDD-2005)* (pp. 678–684).

Stecher, K., & Counts, S. (2008a). Thin Slices of Online Profile Attributes. *ICWSM-2008*. Seattle.

Stecher, K., & Counts, S. (2008b). Spontaneous Inference of Personality Traits from Online Profiles. *ICWSM-2008*. Seattle.

Strater, K., & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, InteractiondVolume 1. BCS-HCI '08* (pp. 111–119). Swinton, UK: British Computer Society.

Strater, K., & Richter, H. (2007). Examining privacy and disclosure in a social networking community. *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security* (pp. 157–158). Retrieved from none

Stutzman, F. (2007). Impression Formation and Management in Social Network Websites. *ICA 2007*. San Francisco, CA.

Stutzman, F., & Kramer-Duffield, J. (2010). Friends Only: Examining a Privacy-Enhancing Behavior in Facebook. *CHI 2010*. Atlanta, GA.

Takahashi, T. (2008). Mobile Phones and Social Networking Sites: Digital Natives' Engagement with Media in Everyday Life in Japan. *Media, Communication & Humanity*. London, England.

Toubiana, V., Narayanan, A., Boneh, D., Nissenbaum, H., & Barocas, S. (2010). Adnostic: Privacy-Preserving Targeted Advertising. *Proceedings of the Network and Distributed System Symposium*. San Diego, California.

Trepte, S., & Reinecke, L. (Eds.). (2011a). *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web*. Heidelberg: Springer Verlag.

Trepte, S., & Reinecke, L. (2011b). The social web as a shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web* (pp. 61–73). Heidelberg: Springer Verlag.

Trere, E. (2008). Privacy and Facebook. Reflections on past, present and future research, proceedings of the conference. *Mobile Communication and the Ethics of Social Networking*. Retrieved from none

Van de Hoven, J. (2008). Information technology, privacy and the protection of personal data. In J. Weckert & J. Van de Hoven (Eds.), *Information Technology and moral philosophy* (pp. 301–321). Cambridge: Cambridge University Press.

Van den Berg, B., & Leenes, R. (2010). Audience Segregation in social network sites. *2010 IEEE Second International Conference on Social Computing* (pp. 1111–1116). IEEE Press.

Young, A. L., & Quan-Hasse, A. (2009). Information revelation and Internet privacy concerns on social network sites: a case study of Facebook. *C&T '09 Proceedings of the fourth international conference on communities and technologies*.

Ziegele, M., & Quiring, O. (2011). Privacy in Social Network Sites. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web* (pp. 175–189). Heidelberg: Springer Verlag.

Government and Industry Reports, Regulations, and Policies

Boyles, J. L., Smith, A., & Madden, M. (2012). *Mobile Privacy and Data Management*. Washington D.C. Retrieved from http://pewInternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf

Center, P. I. R. (2008). *Social Networking and Online Videos Take Off: Internet's Broader Role in Campaign 2008*.

Christofides, E., Muise, A., & Desmarais, S. (2010). *Privacy and Disclosure on Facebook: Youth and Adults' Information Disclosure and Perceptions of Privacy Risks*. Guelph.

DeRosa, C., Cantrell, J., Havens, A., Hawk, J., & Jenkins, L. (2007). *Sharing, Privacy and Trust in Our Networked World*. Retrieved from http://www.oclc.org/reports/sharing/default.htm

European Commission. (2012a). *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Brussels. Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Commission. (2012b). *How will the data protection reform affect social networks?* Brussels. Retrieved from http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

FTC. (2012a). *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy-makers*.

FTC. (2012b). *Mobile Apps for Kids: Disclosures Still Not Making the Grade*. Retrieved from http://www.ftc.gov/opa/2012/12/kidsapp.shtm

FTC. (2012c). *Mobile Apps for Kids Report*. Retrieved from http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

Fuchs, C. (2009). *Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook and MySpace by Students in Salzburg in the Context of Electronic Surveillance*. Vienna.

Hobgen, G. (2007). *Security Issues and Recommendations for Online Social Networks*.

Internet Safety Technical Task Force. (2008). *Enhancing Child Safety and Online Technologies*.

Lenhart, A., Madden, M., & Smith, A. (2007). *Teens, Privacy & Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of MySpace*. Washington.

Livingstone, S., Olafsson, K., & Staksrud, E. (2011). *Social Networking, Age and Privacy*. Retrieved from http://www.eukidsonline.net/

Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). *Social Networking, Age and Privacy*. London, England. Retrieved from http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf

Macgill, A. (2007). *Parent and Teenager Internet Use*. Retrieved from http://www.pewInternet.org/Reports/2007/Parent-and-Teen-Internet-Use.aspx

Madden, M. (2012). *Privacy management on social media sites*. Washington D.C. Retrieved from http://www.pewInternet.org/~/media/Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf

Online Computer Library Center (OCLC). (2007). *Sharing, Privacy and Trust in Our Networked World*. Dublin. Retrieved from http://www.oclc.org/reports/pdfs/sharing.pdf

Smith, A. (2007). *Teens and Online Stranger Contact*. Retrieved from http://www.pewInternet.org/PPF/r/223/report_display.asp

Steeves, V. (2010). *Summary of Research on Youth Online Privacy*. Ottawa.

Storsul, T., Arnseth, H. C., Bucher Taina, Enli, G., Hontvedt, M., Kløvstad, V., & Maasø, A. (2008). *New web phenomena: Government administration and the culture of sharing*.

The White House. (2012). *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Washington DC.

Turow, J., Feldman, L., & Meltzer, K. (2005). *Open to Exploitation: American Shoppers Online and Offline*. Philadelphia.

US Department of Commerce. (2010). *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.