GETTING MORE EXPLICIT ON GENRES OF DISCLOSURE: TOWARDS BETTER UNDERSTANDING OF PRIVACY IN DIGITAL AGE (RESEARCH IN PROGRESS)

Ali Mohammad Padyab
Luleå Tekniska Universitet
Ali.mohammad.padyab@ltu.se

Abstract
Disclosure is all about communication and Genres are about analyzing communicative action. "Genres of Disclosure" as repetitive patterns of disclosing has given less attention. Drawing on Palen and Dourish's work, this paper expand its defined scope from a social approach into a more socio-technical approach. Evolutionized by the affordances of a new digital medium, new genres have emerged. We called these new subgenres, secondary genres of disclosure. We provide a taxonomy for these type of genres and some real examples to illuminate the concept. Implications of use for designing privacy and venues for further research are discussed. It is concluded that "Genres of Disclosure" can serve as a common language between users, system providers and legislators to preserve privacy within any system that has consequences for personal privacy.

Key words: Genre of Disclosure, Genre, Privacy, Disclosure

1. INTRODUCTION

Contemporary information and communication technologies have created new modes of interaction. People now can easily communicate with each other and express themselves with a wide range of people including family, friends, acquaintances or even unknown audiences through different mediums e.g. social media. However once the content goes viral, there can be no guaranty that *only* the intended recipient(s) will receive it. Since 1960's, computational powers led governments and large organizations to gather, analyze and store personal information (Hoffman 1969). First personal computers that were connected to a world wide web opened up new doors to the ocean of valuable user data/metadata by means of tracking user activities (e.g. HTTP cookie) that formed new challenging questions regarding user privacy (Lin and Loui 1998). Nowadays we can see mobile technologies networked together creating inevitable accompanies to comfort one's daily activities. Different factors like adaptation of computing powers, global spread of Internet, affordable devices and etc. in our surroundings has raised concerns regarding public privacy (Rose 1999) in which governments, corporations, companies and other third parties tend to massively collect personal data utilized into behavioral marketing. Privacy heed has risen significantly as a result of different communicative innovations during the past decade (Hoofnagle et al. 2010) and several scholars have warned the effects of advances in information technology on individual's privacy (Nissenbaum 2009, Tene and Polonetsky 2012). Efficiencies in identification, aggregation and mining data have placed businesses and governments in greater power relation than users by circumventing user choice that jeopardizes freedom, safety and relationships (Andrews 2012, Hoofnagle et al. 2012).
Two common pitfalls in designing privacy of a system[1] is to obscuring *actual* and *potential* information flow within a system, which will lead to confusion, breach of privacy and uncertainty (Beckwith 2003, Good et al.

[1] In this paper the notion of system refers to a set of software and hardware designed to allow interaction

2005, Lederer et al. 2004). The participants engaged in a system should be able to clearly see how their information is communicated and the possible ways that their information could be handled. Despite the concerns over the privacy[2], some users are tend to be negligent in protecting their privacy as a result of non-transparency to comprehend where their data go on one hand (Norberg et al. 2007), and we can still see that some privacy safeguards frequently fail (e.g. anonymization (Narayanan and Shmatikov 2009)) on the other hand (Siponen and Vance 2010). User's disclosing behaviors have been the focus of many researchers in order to find different technological solutions that support those. According to Rosenberg, "the best and most effective way to control use of information, without interfering with the conduct of others, is to prevent it from ever coming into others' hands" (Rosenberg 2000, p. 84). Therefore, privacy is directly associated with the way personal information communicated and disclosed from its origin to the intended destination. A disclosure happens when the person initiating the dialog feels that the channel of communication was unfaithful in fulfilling her closure expectations; for instance, personal information falls into wrong hands. Another way to interpret this is what Palen and Dourish (2003) distinguish as *genres of disclosure*. This notion was proposed as a means to investigate the disclosing patterns of communication that is enacted repetitively, it's is recognizable and socially meaningful. Through these genres, a community with a common purpose can understand patterns of disclosure which are similar in terms of structure, style, content and intended audience (Swales 1990). Examples might be talking to a psychiatrist, filling out personal information for registering in a website and writing personal online diaries. Those genres can then be further studied in a privacy affecting system to compare and contrast its abilities against genres of disclosure in determining the extent to which the system coordinate itself with of patterns of "genres of disclosure"; for instance, intended audience within that genre of disclosure is exactly whom the system facilitates interaction to.

Since the first debate by Palen and Dourish more than one decade ago, "genres of disclosure" is still in its infancy. Discussion on implications of genres of disclosure in digital age is still scarce and well-defined complementation of the concept is promised beneficial by scholars like Lederer et al. (2004) who invited designers of privacy persuaded system designers to identify genres of disclosure in order for the users to "(1) understand the extent of the system's alignment with those genres and (2) conduct socially meaningfully action that supports them (or disrupts them, as the case may be)" (ibid, p. 453).

One knowledge gap within privacy literature starts from the point where users are mainly unaware of what is being collected from them due to lack of openness in indicating actual and potential flow of disclosed information by the interacting system (Gadzheva 2007, Lederer et al. 2004). Hence in current literature we could not find any trace of a useful conceptual ground that studies personal information flow and disclosure within a system. Thus the objective of this paper is to answer the question, "what sorts of disclosure patterns available in digital medium and how they could be contributing to personal information privacy?" Digital medium, as the scope of this paper, refers to any system that provides a medium to facilitate user interaction. In order to address this issue we started to look more into communicative patterns of disclosure in a system as a whole other than just looking at the user as an input. This paper is aiming to scrutinize genres of disclosure by expanding its scope in the current literature and to provide taxonomy for the classes of subgenres of the "genres of disclosure" class and implications of this taxonomy in understanding of privacy requirements of a system that could jeopardize personal information.

The reminder of this paper is as follows. First, "genres of disclosure" is discussed based on the current literature. Thereafter follows examples of genres of disclosure by presenting some disclosure practices that occur by normal usage of smart phones. Finally, the paper reexamines the example in detail to conceptualize a new type of genres (i.e. secondary genres of disclosure) and a taxonomy is provided to concretize the concept with discussion and implications of different opportunities for technology development and user's privacy awareness.

[2] There are lot of definitions for privacy but this paper takes the definition from Warren's and Brandeis (1890) "the right to be let alone" (p.193).

2. GENRES OF DISCLOSURE

The concept of genres of disclosure, as the name implies, corresponds to a class of genres where disclosure is conceptualized as a type of communication. In order to understand the term better it is worthwhile to look more deeply at *genres* and *disclosure*.

Genre (from French *genre* and Latin *genus*) means "kind" or "sort" and dates back to the ancient Greek as a classification scheme for the literature. Genres transpired in disciplines and paradigms to interpret human interaction (with the world or human-human) and/or products derived from it (e.g. visual arts). A person acquires language in a patterned way through various genres he is exposed to (Caballero 2008), thus it has shaped our interpersonal abilities in such a way that without it, knowledge of other sorts (e.g. linguistic knowledge) is insufficient for successful interaction (Tomasello 2010). Genres allow us to recognize different items based on their similarity of *content* and *form*. Content refers to motives, logic and themes presented in a communication and Form is a standard unit of communication shaped by linguistic and physical features (Yates and Orlikowski 1992). For example through genre lens, a movie categorized as western is a *type* of movie that is clustered to a certain family that share common features. Although movies of the same genre are different from each other, it makes the comparison of each individual movie much easier.

Disclosure from the literacy meaning is defined as the act of uncovering secret information known. It can be viewed from two perspectives of self-disclosure and unwanted-disclosure. Self-disclosure involves an individual to willingly provide information about the self to others (Jourard and Lasakow 1958) that becomes common knowledge existing between people, within groups or between an individual and another party like an organization. Self-disclosure is seen as a regulator for dynamic interaction which is both the product and process of communication encounter (Ioinson and Paine 2007). Unwanted-disclosure refers to access of a third party to user's information without the user's consent like various types of hacks leading to privacy leakage.

Combination of genre and disclosure therefore refers to types of disclosure that share the same content and form. Genres of disclosure was first debated by Palen and Dourish (2003, p. 133) in 2003 as "socially-constructed patterns of privacy management," or "regularly reproduced arrangements of people, technology and practice that yield identifiable and socially meaningful styles of interaction, information, etc". Central to the concept of genres of disclosure is the adoption of social patterns of expectation and response into recognizable, socially meaningful forms of interaction and information disclosure that genres embody. Social and technical practices will guide and/or affect the social expectations of participants involved in a genre leading to arranging one's patterns of privacy managements. Genres of disclosure draws attention to the communicative practices involved in a system to insinuate about the expectations of use according to the users, therefore designing privacy management in a system keeps up with the promise of genre (i.e. expectation of use). For example disclosing credit card information to an online store during check out is a commonly understood type of communication that differs from traditional ways of paying (e.g. with cash in a physical store). It requires a user to reveal some digits, name and last name via a computer mediated device. This genre of disclosure raises concerns about the usage of this information in which failure to those expectation will guide the user's privacy managing arrangement to corporate or defy with that genre. From system designer's perspective, providing mechanisms aligned with expectation of use will ensure that disclosed content will not misappropriated and used unpredictably.

The genres enumerated so far thus candidate users as sources of disclosure. However in this paper it is argued that digital medium has other sources of disclosure. The following section will examine a simple case of smart phone use and then we scrutinize the example to inspect different genres of disclosure.

3. EXAMPLE

Advances in telecommunication industry have turned the fashioned simple mobile phones into sophisticated devices with strong computational powers. It is so proliferated that it has become part of our lives. They are no more an only-call-messaging device but features embedded and device portability improved so that users

can now more easily access useful information anywhere through sophisticated interactive applications. Each device benefits from significant hardware developments such as positioning, sensing, wireless communications, camera and global networking. Smartphones contain a fistful of personal information like contact list, call history, SMS, photos, emails and etc. A simple usage of smartphone involves a wide range of disclosing activities initiated by different parties.

Enforced by their own regulatory practices of privacy management, users deliberately adjust their level of disclosure based on information they use to communicate, purpose of communicative action, to whom are they communicating with, time of communication, the place of the communication take place (Lederer et al. 2004, Yoshioka et al. 2001). This will allow them to create situation of expectation and response among the people prompt disclosure of certain information according the abovementioned circumstances. For example one person calling a "Telephone Banking" service activates some patterns of communication different than other calling practices. In this case, a person expects to reveal identity number and pin code to the bank system via phone when she needs to handle general banking activities e.g. to check her account balance.

Another example is the usage of applications within smartphones. Apps need to access user's data (e.g. location, contacts, Wi-Fi SSID) available via the smartphone to implement their core features accordingly. Using an application requires permission from users agreeing to disclose their information with that application. Therefore based on this genre of disclosure, users should adjust their preferences under their social practices of disclosure at some particular time, some particular place, whom should see it, what content can be concealed.

Once the use agrees to use that smartphone or disclosed data transferred from her, a range of technologies can facilitate exploitation of personal information. For example it was released (Valentino-DeVries and Angwin 2011) that Google's Android and Apple's iOS, two popular OSs in smartphones, regularly transmit their locations back to Apple and Google. Location services in smartphones are used for different purposes, allowing users to use applications like maps and social media. However according to the report the location information appeared to be transmitted even when there is no application running. It was also found that coordination was also tied with device's Unique ID number (location then acts as metadata for UID). There have been some reports showing that some applications have used location services without user's consent or knowledge (Thurm and Kane 2010, Zhou et al. 2011).

Another example is the usage of user data beyond interacting system's knowledge. Edward Snowden is recognized as the whistleblower of the most significant leaks in US political history, on National Security Agency (NSA)'s surveillance program (Greenwald et al. 2013). In one of his revelations, Snowden presented documents on NSA's program on infiltrating into systems of Internet giants Google, Apple, Facebook and others. By penetrating the data links between these corporation's datacenters, NSA were able to collect material including email, video and voice chat, videos, photos, voice-over-IP (Skype, for example), chats, file transfers, social networking details, and more (Greenwald and MacAskill 2013). Those system providers have denied any knowledge about the NSA's programs and denied any collaboration.

In a similar attempt related to our case of mobile phone usage, according to the leaked documents NSA is gathering the whereabouts of cellphones around the world. With the purpose of tracking every movement of individuals and connection between people, NSA developed sophisticated methods of tracking and various analytic techniques (Gellman and Soltani 2013). One technique is called "Co-traveler Analytics" which makes it possible to spy on an intelligent target's phone and their co-travelers using data gathered from cellular towers.

As mentioned in this example, disclosure can evolve at two levels: 1) where service providers are the strategic beneficiary and 2) where service providers are being encroached upon.

4. DISCUSSION AND CONCLUSION

Looking at the previous example through genre glass, we can see that there is one more type of information disclosure that could be defined under "genres of disclosure" realm. Those genres have unique characteristics

that need to be considered as separate type of "genres of disclosure" that is defined under current literature. This section deals with this type and explains its existence from genre perspective.

The emergence of the electronic medium has opened up new ways of interaction that is evolving very fast by the new development in Information and Communication Technologies (ICT). New genres may emerge (e.g. according to the advancements in ICT) whenever demands for new communicative patterns becomes incumbent (i.e. "hybrid") (Fairclough 1993). As pointed out by literary scholar Todorov (1990, p. 15) when asking: "Where do genres come from? Quite simply from other genres. A new genre is always the transformation of an earlier one, or of several: by inversion, by displacement, by combination". However this viewpoint is not always true for the genres mediated by ICT i.e. *cybergenres*. Although some cybergenres inherit from their offline counterparts (e.g. VoIP calls), others tend to emerge due to the features of communication medium (e.g. selfie) uniquely characterizing a new genre. Genre transformation and emergence of novel genres in ICT ecosystem (the combination of computers, telecommunications, the Internet, and media) has been under study of many researchers. Shepherd and Watters (1998) underlined the evolution of cybergenres and found that online genres are classified into two subclasses of 1) *Extant* genres, that are either replication or maturation of offline genres with some small changes enforced by the new medium, and 2) *novel* cybergenres, which are transmuted (or generated) to the extent which they are considered as fairly new genres. These genres are unique and only exist because of the new features in the medium.

The electronic technologies and media have given rise to the new genres (and naturally genres of disclosure). One unique characteristic of digital genres that makes them a distinguishable class of genres is *functionality*, referring to the new capabilities offered by the new medium (Crowston and Williams 2000, Shepherd and Watters 1998). Mediated by technological improvements of ICT, these digital genres will make new possibilities in terms of functions that engaged parties in a communication can actually do. Consequently these functionalities introduce new subclasses of genres of disclosure that goes beyond Palen and Dourish's "socially-constructed patterns of privacy management" definition. Here we argue that genres of disclosure is no longer just "recurrent social practices" but there are some intrinsically capabilities of disclosure in a digital communication that one's disclosing and "socially meaningful styles of interaction" is not yet fully what she is participating into. We would expand this notion of "genres of disclosure" from its solely user's subjective point of view (referred to as 'user's genres of disclosure' in this paper) into a more socio-technical perspective. By this we mean that in a system that facilitates interaction for its users, there are some technological artifacts that breed functionalities of new genres of disclosure. We refer to these genres that are mediated by technological artifacts, targeted at breaching user information beyond user's privacy management regulations, as **secondary genres of disclosure**. Figure 1 depicts a system where users are interacting through different genres of disclosure illustrated by different arrows with different colors to resemble each unique genre i.e. repetitive practices of information disclosure. In these first-hand communications a person will justify the system's affordances to meet her roles, expectations, responses and practices. At this stage the system anticipates user's genres of disclosure and translates those genres into elucidative practices through different technological instruments (e.g. user expects to communicate securely during online banking and system obliges that by providing SSL). Secondary genres of disclosure take place during or after primary disclosing practice where users (and targeted system at some points) are unaware of happening disclosing action. The arrows illustrated in the secondary genres are two way, meaning that targeted system either deliberately discloses those info or subconsciously. The triggering force to initiation of this action is the functionalities of the system itself that might lead to further exploitation of genre. Here secondary genres are not only regarded as models or prototypes of human communication (Paltridge 1997), as user's genres may imply. Although secondary genres could be regarded as social practice between system providers and third parties, but also as what Saville-Troike (1982) refers to 'type of event'; takes place to accomplish in the particular, recurrent situation (Miller 1984), in this case the action of mining personal information by the system itself or stealing by other third parties.

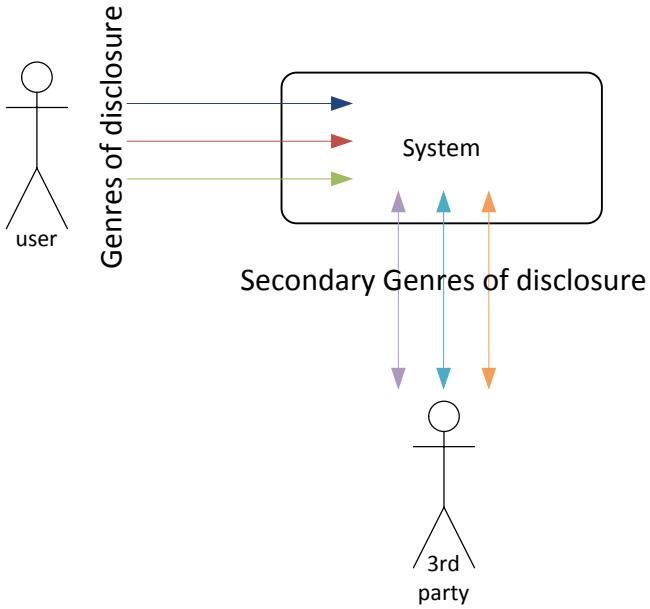

Figure 1 taxonomy for genres of disclosure

The point of departure from our definition of genres of disclosure than of Palen and Dourish's is when content is digitalized and genre takes the functionality element as its characteristic[3]. Then the user has little or no control over the disclosed information. Once communication established within the system, a range of secondary genres of disclosure emerge either inherited by their offline counterparts or spontaneously. For instance in the previous example, NSA were able to exploit the functionalities of mobile technologies to infiltrate into people's personal information when they were using their mobile phones. Disclosure could be due to deliberate collection, selling and trading of data by the interacting system itself (Gomez et al. 2009) or exploitation from third parties by infiltrating into the system (Ghernaouti-Hélie 2012). What justifies the collection of personal data is their strategic importance for favorable or mischievous purposes (Hirsch 2010). As noted by Federal Trade Commission, "…businesses have always collected some data from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of unprecedented amounts of data that can be used for **myriad subsequent purposes**" (Federal Trade Commission 2000, p. 33). Therefore we imply that secondary genres of disclosure have one more element of "intention" to be able to qualify as this type of genres; i.e. to be identified as an unique genre. Here "intention" insinuates to beneficiary's purpose to exploit user's aggregated data in order to gain strategic knowledge. According to Bhatia (1999) genres may have one main purpose and several sub-purposes. In these secondary genres of disclosure the main purpose is "strategic knowledge" and subordinate purposes are exactly what the element of "intention" is trying to capture. For example a website may gather their visitor's data with the purpose of strategic advantage (main purpose) but disclosing it to their contractor for the purpose of website improvement (intention) or sell (intention) the data to the advertising companies.

Recalling the examples of smart phone use in the previous section will reveal a number of secondary genres of disclosure. Collection of user location by Apple and Google can now be interpreted as an unique genre. They employed technological affordances of GPS enabled devices to gather latitude and longitude of users to build giant databases of Internet Wi-Fi hotspots. We call this genre "gathering user's location data" which implies a recurrent type of communication aimed at building location based services by Apple and Google. Other usage of this type of genre was interception of Internet giant's datacenters by NSA. From genre perspective, user's various information which was supposed to kept secret including chat logs, voice, video,

[3] Since in this paper we are only targeting ICT mediated genres of disclosure, therefore functionality is an embedded element of this type of digital genres. However there could exist other types of genres of disclosure that are offline (e.g. face to face doctor-patient meeting) but it is not our intention to discuss them in this paper.

location and etc were seized through communication lines of service providers. With the purpose of profiling people, this reparative act of profiling is composed by different characteristics which make it a different type of disclosing pattern of communication than of e.g. profiling by data brokers. Here the difference lies within purpose, content, form and functionalities of digital medium that facilitate the disclosure.

In this paper we have shed more light on the concept of "Genres of Disclosure" as a mean to study privacy in today's digital world. We argued that *Disclosure* is essentially about communication and *Genres* provides grounds to conceptualize communication patterns. Drawing of Palen and Dourish's (2003) "Genres of Disclosure" we expanded the concept from a social perspective on privacy into a more socio-technical view.

Lederer et al. (2004) emphasized on five pitfalls to heed when designing for privacy. Two of those common problems among system designers are blurring disclosed *actual* and *potential* information flow that can affect user's understanding of a system's privacy implications. The genre lens has been regarded as a useful means for analyzing communicative practices and information systems (Orlikowski & Yates, 1994). In this paper we argue that genres of disclosure can alleviate those pitfalls by concretizing established patterns of interaction and communication that is already open for interaction and indicating the potential channels that could seep information. Genre approach gives grounds as a basis of identifying information sharing/breaching situations and mapped genres could be employed for further analysis of security breaches (Padyab et al. 2014).

In the proposed taxonomy, genres of disclosure can inform the users about what is actually being shared and disclosed. It can have implications at three levels:

- In line with user's genres of disclosure, since users are conduits of disclosure, system designers can learn about use's expectations and responses with a resultant system through genres. This can lead to contrive sufficient technical mechanisms which will make sure users are able to put their subjective privacy regulation into practice.
- Secondary genres of disclosure can make service provider's system more transparent to the user with higher fidelity. It will also allow users to be more aware of the whereabouts of their information as it traverses through the system to opt in or out of those genres of disclosure. Since genres are either reproduction of past genres or emerge as new one, system providers by studying those genres that currently available offline and features of a new medium can prevent those extant genres.
- Policy makers drawing on those genres might be able to create educational programs about disclosure practices and make user's informed about their disclosing practices.

Genre theory and it basic concepts seems to serve as a basis of analyzing communication especially within the public and private domains. Scrutinizing of interests between public and private spheres makes the basis for privacy (Arendt 1958) and genre thinking gives fundamental conceptual ground to proactively identify and understand privacy/transparency risks by incorporating user's normative behavior into further developments to "pursue the principles of the ideal speech situation in communication" (Habermas 1984, Päivärinta 2001). Genres of disclosure can foster more discussion on Habermas' strategic versus emancipatory interest of different stakeholders (Habermas 1984) but this paper suffices to just mention about its potential and in subsequent papers we will discuss more about this.

This article is a research in progress and it will require further work to reach maturity. Limitation of this work lies within its presentation of highly abstract concepts which lacks demonstration of practicality. The examples presented here are bound with secondary data and it needs to be strengthened with data gathered in a real setting. Further research could address how genres could be captured in real practice. Genres, in practice pose some challenges that need to be addressed. For instance it is considered as a cumbersome task, since there might be so many genres a system (Padyab et al. 2014, Päivärinta 2001). Building on this article, we will explore the genres of disclosure together with users and system designers in the future work.

5. Acknowledgement

This work was funded by the European Commission in the context of the FP7 ICT project USEMP (under grant no: 611596) and EIT ICT Labs under project name REAL-TIME SECURITY SHIELD FOR MOBILE PLATFROMS.

6. REFERENCES

Andrews, L. 2012. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*. Simon and Schuster.

Arendt, H. 1958. *The human condition*. University of Chicago Press.

Beckwith, R. 2003. Designing for ubiquity: the perception of privacy. *IEEE Pervasive Comput*. **2**(2) 40–46.

Bhatia, V. K. 1999. Integrating products, processes, purposes and participants in professional writing. C. Candlin, K. Hyland, eds. *Writ*. *Texts Process*. *Pract*.. London & New York, Longman, 21–40.

Caballero, R. 2008. Theorizing about genre and cybergenre. *CORELL Comput*. *Resour*. *Lang*. *Learn*. **2** 14–27.

Crowston, K., M. Williams. 2000. Reproduced and Emergent Genres of Communication on the World Wide Web. *Inf*. *Soc*. **16**(3) 201–15.

Fairclough, N. 1993. *Discourse and Social Change*. Wiley.

Federal Trade Commission. 2000. *Privacy online fair information practices in the electronic marketplace : a report to Congress*. DIANE Publishing. Available at: http://goo.gl/NxhlWP.

Gadzheva, M. 2007. Privacy in the Age of Transparency: The New Vulnerability of the Individual. *Soc*. *Sci*. *Comput*. *Rev*. Available at: http://ssc.sagepub.com/content/early/2007/12/03/0894439307307686 [Accessed July 3, 2014].

Gellman, B., A. Soltani. 2013. NSA tracking cellphone locations worldwide, Snowden documents show. *Wash*. *Post*. Available at: http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html [Accessed June 30, 2014].

Ghernaouti-Hélie, S. 2012. The Cybercrime Ecosystem & Privacy Issues - Main Challenges and Perspectives from a Societal Perspective. *ERCIM News* (90).

Gomez, J., T. Pinnick, A. Soltani. 2009. *KnowPrivacy*. Available at: http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

Good, N., R. Dhamija, J. Grossklags, D. Thaw, S. Aronowitz, D. Mulligan, J. Konstan. 2005. Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. *Proc*. *2005 Symp*. *Usable Priv*. *Secur*.. SOUPS '05. New York, NY, USA, ACM, 43–52. Available at: http://doi.acm.org/10.1145/1073001.1073006 [Accessed June 30, 2014].

Greenwald, G., E. MacAskill. 2013. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Available at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [Accessed June 28, 2014].

Greenwald, G., E. MacAskill, L. Poitras. 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*. Available at: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [Accessed June 28, 2014].

Habermas, J. 1984. *The Theory of Communicative Action: Reason and the rationalization of society*. Beacon Press.

Hirsch, D. D. 2010. The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation. *Seattle UL Rev* **34** 439.

Hoffman, L. J. 1969. Computers and privacy: A survey. *ACM Comput. Surv. CSUR* **1**(2) 85–103.

Hoofnagle, C. J., J. King, S. Li, J. Turow. 2010. *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*. Rochester, NY, Social Science Research Network. Available at: http://papers.ssrn.com/abstract=1589864 [Accessed June 8, 2014].

Hoofnagle, C. J., A. Soltani, N. Good, D. J. Wambach, M. Ayenson. 2012. *Behavioral Advertising: The Offer You Cannot Refuse*. Rochester, NY, Social Science Research Network. Available at: http://papers.ssrn.com/abstract=2137601 [Accessed June 3, 2014].

Ioinson, A. N., C. B. Paine. 2007. Self-disclosure, privacy and the Internet. *Oxf. Handb. Internet Psychol.* 2374252.

Jourard, S. M., P. Lasakow. 1958. Some factors in self-disclosure. *J. Abnorm. Soc. Psychol.* **56**(1) 91–98.

Lederer, S., J. I. Hong, A. K. Dey, J. A. Landay. 2004. Personal privacy through understanding and action: five pitfalls for designers. *Pers. Ubiquitous Comput.* **8**(6) 440–454.

Lin, D., M. C. Loui. 1998. Taking the Byte out of Cookies: Privacy, Consent, and the Web. *Proc. Ethics Soc. Impact Compon. Shap. Policy Inf. Age*. ACM POLICY '98. New York, NY, USA, ACM, 39–51. Available at: http://doi.acm.org/10.1145/276755.276775 [Accessed June 7, 2014].

Miller, C. R. 1984. Genre as social action. *Q. J. Speech* **70**(2) 151–167.

Narayanan, A., V. Shmatikov. 2009. De-anonymizing Social Networks. *2009 30th IEEE Symp. Secur. Priv.*. 173–187.

Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Norberg, P. A., D. R. Horne, D. A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *J. Consum. Aff.* **41**(1) 100–126.

Padyab, A. M., T. Paivarinta, D. Harnesk. 2014. Genre-Based Assessment of Information and Knowledge Security Risks. *2014 47th Hawaii Int. Conf. Syst. Sci. HICSS*. 3442–3451.

Päivärinta, T. 2001. The concept of genre within the critical approach to information systems development. *Inf. Organ.* **11**(3) 207–234.

Palen, L., P. Dourish. 2003. Unpacking privacy for a networked world. *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*. ACM, 129–136. Available at: http://dl.acm.org/citation.cfm?id=642635 [Accessed April 17, 2014].

Paltridge, B. 1997. *Genre, Frames and Writing in Research Settings*. John Benjamins Publishing.

Rose, N. 1999. *Powers of Freedom: Reframing Political Thought*. Cambridge University Press.

Rosenberg, A. 2000. Privacy as a Matter of Taste and Right. *Soc. Philos. Policy* **17**(02) 68–.

Saville-Troike, M. 1982. *The Ethnography of Communication: An Introduction*. Blackwell.

Shepherd, M., C. Watters. 1998. The evolution of cybergenres. *Proc. Thirty-First Hawaii Int. Conf. Syst. Sci. 1998*. 97–109 vol.2.

Siponen, M., A. Vance. 2010. Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *MIS Q* **34**(3) 487–502.

Swales, J. 1990. *Genre Analysis: English in Academic and Research Settings*. Cambridge University Press.

Tene, O., J. Polonetsky. 2012. *Big Data for All: Privacy and User Control in the Age of Analytics*. Rochester, NY, Social Science Research Network. Available at: http://papers.ssrn.com/abstract=2149364 [Accessed June 8, 2014].

Thurm, S., Y. I. Kane. 2010. Your Apps Are Watching You. *Wall Str. J.* Available at: http://online.wsj.com/news/articles/SB10001424052748704368004576027751867039730?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704368004576027751867039730.html#ixzz18WFHX4pP [Accessed June 28, 2014].

Todorov, T. 1990. *Genres in Discourse*. Cambridge University Press.

Tomasello, M. 2010. *Origins of Human Communication*. Mit Press.

Valentino-DeVries, J., J. Angwin. 2011. Apple, Google Collect User Data. *Wall Str. J.* Available at: http://online.wsj.com/news/articles/SB10001424052748703983704576277101723453610?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748703983704576277101723453610.html [Accessed June 28, 2014].

Warren, S. D., L. D. Brandeis. 1890. The Right to Privacy. *Harv. Law Rev.* **4**(5) 193–220.

Yates, J., W. J. Orlikowski. 1992. Genres of Organizational Communication: A Structurational Approach to Studying Communication and Media. *Acad. Manage. Rev.* **17**(2) 299.

Yoshioka, T., G. Herman, J. Yates, W. Orlikowski. 2001. Genre Taxonomy: A Knowledge Repository of Communicative Actions. *ACM Trans Inf Syst* **19**(4) 431–456.

Zhou, Y., X. Zhang, X. Jiang, V. W. Freeh. 2011. Taming Information-Stealing Smartphone Applications (on Android). J. M. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, A. Sasse, Y. Beres, eds. *Trust Trust*. *Comput*.. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 93–107. Available at: http://link.springer.com/chapter/10.1007/978-3-642-21599-5_7 [Accessed June 28, 2014].