

PRIMA¹ — Privacy Research through the Perspective of a Multidisciplinary Mash up

Markus Bylund
Mikael Johnson
Asko Lehmuskallio
Peter Seipel
Sakari Tamminen

Abstract

Based on a summary description of privacy protection research within three fields of inquiry, viz. the social sciences, legal science, and computer and systems sciences, we discuss multidisciplinary approaches with regard to the difficulties and the risks that they entail as well as their possible advantages. The latter include the identification of relevant perspectives of privacy, increased expressiveness in the formulation of research goals, opportunities for improved research methods, and a boost in the utility of invested research efforts.

1 PRIMA is funded by the Nordic Council of Ministers through the Nordic University Network (NORDUNET). The main active partners are the Swedish Institute of Computer Science, SICS (coordinator); the Software Business and Engineering Institute, Helsinki University of Technology (TKK); the Tampere Unit for Computer-Human Interaction, University of Tampere; and the Law and Informatics Research Institute (IRI), Stockholm University.

1 Introduction

Right from the early days of electronic data processing in the 1960s, the protection of the privacy of data subjects has been an issue. Over the decades, it has become both more far-reaching in terms of societal consequences and more complex in terms of definitions, contexts, technology, stakeholders, and so forth. Today, privacy is a prime component of almost every discussion of the networked information society. Not surprisingly, privacy was chosen as one of the workshop topics at the e-Stockholm '08 Legal Conference in November 2008. The workshop was based on ongoing activities in a Nordic research project, Privacy in the Making (PRIMA). In this paper, we discuss modern privacy protection research in the light of PRIMA and the e-Stockholm workshop. In particular, we pay attention to multidisciplinary approaches to privacy protection.

1.1 The Maze of Approaches to Privacy

Discussions about privacy protection tend to raise the question of whether the participants are talking about the same thing. Not least, such confusion may occur when experts with different theoretical backgrounds come together and each one of them is not at all or only peripherally aware of the worldviews and methodological orientations of the others. For example, the legal expert may find it difficult to relate traditional, legal reasoning about privacy to anthropological studies of user behavior in the tradition of the social sciences. The concepts used, the goals to be achieved, the priorities, the literature cited, can all appear unfamiliar and be experienced as stumbling stones rather than an aid to understanding. And the lawmaker's efforts to transform the results of opinion polls into regulatory solutions can at best be described as problematic.

The notion of privacy is in itself multifaceted and elusive. Its historical roots are to be found in a variety of cultural, social, technical, and economic settings. They range from deeply embedded biological strivings and factors, such as the strive for self-preservation and self-control, to cultural phenomena such as attitudes, desires and expectations. Not least, privacy and the protection of privacy must be described as a highly dynamic phenomenon. This means, among other things, that the notions of privacy change over time, that privacy is context-dependent (not least with regard to different cultural practices), and that the urge for privacy protection may be both emotional and rational.

1.2 Multidisciplinary Efforts to Chart Privacy Issues

Issues of privacy protection have since long been approached from different angles. For example, many studies seek to chart people's views of the need for protection, their actual behavior in privacy-sensitive settings, the shape and usefulness of various privacy-enhancing technologies (PETs), and the shape of privacy policies in different types of activities. Some of these activities are by now well-established (e.g., surveys of privacy concerns) whereas others are speculative and at an early stage of development (e.g. privacy-related research in neurobiology). Generally speaking, most research projects stay within the confines of a particular approach and do not aspire to a broadened understanding of different ways of viewing the subject and how these relate to one another.² In some recent research projects (e.g., the EU FP7 funded PRIME project, <http://www.prime-project.eu>), elements of multidisciplinary work have been included.

Concerns such as these have been central in the design and carrying out of two particular research projects that form the background for this article. In sum, the main purpose of these projects was to probe the design and usefulness of multidisciplinary approaches to privacy protection.

The preceding SAITS project took place during 2002-2005.³ Among the conclusions of SAITS, it may be noted is that multidisciplinary work requires a relatively long learning period and careful planning to achieve coordinated application of different perspectives. Another conclusion is that a multidisciplinary strategy appears to be an essential precondition for the development of practical solutions to privacy protection problems in the complex world of ubiquitous computing and global data networks.

The PRIMA (Privacy in the Making) project began its activities in autumn 2006 and will run until spring 2010. Like in the SAITS project, a multidisciplinary structure is a main attribute of PRIMA and efforts are made to develop combined and shared models for the study of privacy protection. The privacy protection issues under study range from concerns caused by particular privacy sensitive technical equipment (e.g., tools to be used for eye gaze tracking and RFID technology) to studies of people's attitudes and the mindscapes relevant in the privacy context. In other words, the various research

2 For an illustration of the various concerns regarding perspectives, see Iachello & Hong (2007), chapter 2 "The Privacy Landscape".

3 The acronym stands for key letters in the Swedish name of the project (Skydd av användare i informationssamhället – Protection of Users in the Information Society). SAITS was funded by The Swedish Governmental Agency for Innovation Systems (Vinnova). The project was coordinated by the Swedish Institute of Computer Science.

activities give examples of both *hard* and *soft* orientations. The legal issues are correspondingly complex and involve not only traditional and formal analyses of existing regulation but also, e.g., issues of alternative ways of dealing with risks of infringement. The latter presupposes both practical studies of such risks and efforts to develop standardized tools to deal with them (e.g., ways of creating intimacy on networked meeting places). In November 2008, PRIMA was presented at the e-Stockholm '08 Legal Conference on IT Regulations and Policies. The multidisciplinary workshop gave an opportunity to clarify and debate present-day privacy protection concerns (Seipel 2009). The workshop focused both on general issues such as what is privacy and what are the main concerns, and on particular aspects of privacy such as the situation for children. The outcome was not a shared, common understanding of how privacy protection research ought to be conducted (e.g., goals, priorities, and definitions) but rather a vivid experience of the difficulties of reaching an agreement of this sort.

1.3 A Rationale for a Multidisciplinary Perspective of Privacy

The experiences of the above-mentioned projects indicate strongly the importance of fostering an awareness of the many different aspects of privacy protection and an understanding of how they tie together. A rough list of some central concerns includes:

- Rational lawmaking strategies, e.g., securing that regulation functions well in practice (the problem of paper laws).
- Technical design methods and strategies, e.g., the management of identities and anonymity.
- Matters of mental health and comfort, e.g., growing up in a digital world.
- Human rights concerns, e.g., collisions between different fundamental rights and how to avoid them.
- Markets and economic concerns, e.g., behavioral advertising.
- Democratic concerns, e.g., various kinds of digital divides.

Given these concerns and their call for an increasingly sophisticated understanding of privacy and privacy protection, it may be said that the classical “right to be let alone” (Warren & Brandeis 1890) remains valid but must be placed in a modern setting where it has to co-exist with people’s interests in a networked life. The traditional basic principles of privacy protection laws (such

as *the purpose specification principle*) are still useful but are in need of rethinking. We argue that the key to such rethinking requires orchestrated multidisciplinary.

2 Three Perspectives

Three areas of research are represented in PRIMA, viz. the social sciences, law, and computer and systems sciences. More precisely, the orientation as far as the social sciences are concerned may be described as focusing mainly on work done in sociology, social psychology, anthropology, philosophy, and communication studies. As regards law, focus is on data protection law in a broad sense and legal informatics. The latter is in itself multidisciplinary in nature and one of its main themes concerns the interaction of law and IT (Seipel 2002). In computer and systems sciences, privacy is regarded as a design objective. However, the perception of privacy within the field varies substantially, and thus the strategies employed to achieve privacy-friendly systems.

The summaries that follow are intended to give nutshell descriptions of the research areas at issue as they are presently understood. They reflect the discussions within the PRIMA group, which have often been aimed at mutual basic education about the other party's knowledge bases, research interests, and methods in order to further multidisciplinary privacy-related research.

2.1 Setting the Stage

The idea that certain parts of human life can claim special respect and should be granted protection can be traced far back (see Section 2.3). The shape of this idea has continuously changed and developed due to conditions of life, political fashions and convictions, philosophical theories, religious beliefs, individual attitudes, and so forth. The theoretical study of the phenomenon under the concept of privacy is more recent. As for legal science, an article in the 1890 issue of the Harvard Law Review by Samuel Warren and Louis Brandeis, "The Right to Privacy", is usually cited as a seminal work in Anglo-American common law (see, e.g., Bygrave 2002, p. 128; Warren & Brandeis 1890). In Sweden, like in many other countries, attempts in the same direction were relatively few and scattered. The early works played a significant role by analyzing and interpreting central problems of privacy protection, not least the balancing of interests that is an intrinsic element of a right to privacy.

The modern era of privacy protection studies, which is heralded in the Warren and Brandeis' article, begins in the mid 20th century with the rapidly growing use of computers in society. What happens is that the traditional perspective of a right to be let alone becomes increasingly perceived as too narrow. Data protection and the design and use of data processing systems become important topics. Generally speaking, needs occur for a better understanding of an expanding and more complex notion of privacy protection. Typically, it has to do with an interest in information systems and the many activities that they provide space and instruments for. A rather typical reference to such needs can be found in a study of Iachello & Hong where they discuss, among other things, the reasons for human-computer interaction researchers to care about privacy:

“Like ‘usability’ and ‘security,’ privacy is a holistic property of interactive systems, *which include the people using them*. An entire system may be ruined by a single poorly implemented component that leaks personal information, or a poor interface that users cannot understand” (Iachello & Hong 2007, p. 5).

The need for a broad understanding of privacy is also reflected in the recommendations of a RAND Europe study in 2009 (Robinson et al.). With regard to the Independent Supervisory Authorities (ISA) that administers national data protection laws the report states that:

“In any respect, ISAs must evolve from being focused upon process and legal checking, to a broader advisory and enforcement role. This will mean that their staffing requirements will include economists, behavioral scientists and sociologists as well as legal experts and those with practical experience of data protection and privacy issues in public and private contexts” (op. cit. p. 58).

2.2 Social Sciences

One of two main discussions on privacy in the social sciences relates to the distinction between private and public spheres of communal life. Going back to the earliest philosophical debates, the idea of separating politics (public) from the domestic sphere (private) has been a leading idea in the assembly of ideal forms of society (Arendt 1958). Later, the separation between politics (public) and economy (a second approach to make a distinction between the public and the private, as e.g., in private banking) has become a key issue in the constitution of social life (Habermas 1962, Sennett 1977). In other words, the classical discourses on privacy relate to the role of politics and the state in guiding individual action and thus organizing societal life. The distinction

between public and private has been criticized by writers who stress the partiality of public politics and the asymmetrical power structure in the private. Especially feminist scholars have underscored that the private is political and is a good starting point for understanding societal power relations, whereas the public is ever more dispersed into various distinct public spheres (Fraser 1993; Appadurai 1996; Crossley 2004). These discussions and their legacy are visible in one of the two main contemporary social science approaches to privacy: *privacy as a value*.

Acknowledging this background, value-based privacy discussions operate on a macro-societal level. Here, privacy is tied to discussions of human rights and the organizational structure of societies. This is why different value-based privacy paradigms compete with each other, depending on the view of an ideal society. A libertarian perspective stresses the importance of privacy for enabling self-realization, thus granting individuals control of their own lives while limiting Governments' arbitrary power over it (e.g., Locke 1960; Westin 1967; Rössler 2005). In contrast, a communitarian perspective does not regard individual self-realization as important as pursuing a common good; this limits individual liberties in favor of communitarian ones (e.g., Etzioni 1999; 2004). Later authors reply that the value of individual privacy is not mainly a personal phenomenon, but a collective and egalitarian value, since it enables freedom of association and speech, as well as delimits discriminatory practices based on collective differences such as age, gender, ethnicity, religiosity, and political affiliation (e.g., Regan 1995; Bennett & Raab 2006). These perspectives are tightly interlinked with philosophy and sociology of law.

The second main approach to privacy in the social sciences analyses privacy in social interaction between individuals. This approach has two variations: *privacy as a categorical phenomenon*, and *privacy as a boundary regulation and negotiation process*. These interpersonal approaches focus on a more micro-societal level of analysis. Here, privacy is understood to emerge in the context of social relationships, where it is woven into interdependent social action. As such, privacy is seen either as a categorical phenomenon with specific functions (Westin 1967; 2003) or as a constant ongoing boundary regulation and negotiation process (Altman 1975). Categorical approaches stress that privacy can be identified by social-psychological states such as solitude, intimacy, anonymity, and reserve (Westin 1967, 2003; Marshall 1974; Craddock 1997; Pedersen 1996). Boundary regulation, in contrast, does not identify psychological states, but rather ideal ones (desired vs. achieved privacy). Because privacy is a constant optimization process within countless interactions in everyday life, it is possible to identify different boundary regulation mechanisms that individuals, groups, and organizations use in their mutual interactions (Margulis 2003). These involve, e.g., personal disclosure and temporal boundaries, mediated by physical as well as digital mechanisms

(Petronio 2002). These theories have influenced both quantitative privacy studies using questionnaires and more qualitative approaches.

The question of the universality and possible cultural variation of privacy has given birth to studies that have compared answers to similar questions asked in various countries. In an early study, Altman (1977) collected ethnographic evidence from field reports in order to support his thesis that privacy is culturally universal but regulated differently in different parts of the world. Others again, in collecting first-hand empirical data, have been surprised by the similarity of the reasons that interviewees have given for their privacy reasoning (e.g., Newell 1998). Nevertheless, people in different countries tend to have varying levels of trust in government authorities and businesses; some showing a high degree of trust towards these actors, whereas others tend to be more critical. A variety of studies suggest that people within specific state boundaries tend to have different approaches towards privacy and self-disclosure, classified originally by Westin as “privacy fundamentalists”, that is the concerned ones, the “pragmatists”, and the “unconcerned” (for an overview of Westin’s studies see Kumaraguru & Cranor 2005). Looking at cross-national privacy differences from a boundary regulation perspective, it is nevertheless evident that the mechanisms used in order to regulate privacy differ dramatically in different settings. For example, Muslim women in Saudi Arabia tend to have different mechanisms for their privacy regulation than Shintoist women in Japan.

Recently further elaborated social theories, e.g., *actor network theory* (Callon 1986; Latour 1987; Law & Mol 2002), *symbolic interactionism* (Blumer 1969; Bowker & Star 1999; Clarke & Star 2003; Clarke 2005), and *activity theory* (Engeström et. al 1999; Kaptelinin & Nardi 2006) complement the previous discussions of privacy by underscoring the importance of material conditions in the constitution of social interaction. The research has focused on how different material infrastructures make particular forms of interaction possible in the first place, and how these mediate social interaction in, e.g., IT environments (digitalized forms of interaction and the interaction patterns that they entail). Material infrastructures are seen to have an agency of their own in molding the ways in which we relate to each other. In the networked world that we live in today, much of the interaction of our everyday lives takes place in settings that used to require face-to-face interaction – e.g., through email, instant messaging and social networking sites. These new digital means of interacting with each other also change the practical forms of social interaction and trails left behind of any conversation carried out. The new social theories, such as the ones listed above, are helpful in analyzing, conceptualizing, and explaining how privacy emerges as an issue in today’s digital-material infrastructures and networks as well as how people perceive and deal with what has become *obligatory points of passage* in our everyday interaction.

2.3 Law and Legal Informatics

Recently, a legislative committee presented a survey of Swedish privacy protection legislation.⁴ The two-volume study maps existing regulations according to, e.g., varying scope, purpose, and area of law. The survey clearly illustrates that the subject matter is complex as well as wide-ranging. All in all, the Committee's analysis comprises about 1,000 pages. The situation in other nations is more or less similar. In addition to what may be called *core regulations* such as laws on protection of private life, protection of personal data, and secrecy obligations of certain professionals, there is a broad *outer region of laws* and regulations that are more indirectly associated with privacy protection. Copyright legislation can be mentioned as one example; note, among other things, the author's personal rights (*droit morale*) in a work as opposed to the economic rights. Also note that the regulation to be considered encompasses not only statutory subject matter and case law, i.e. binding legal norms in the strict sense, but also other kinds of norms of varying formal nature, suffice it to mention codes of conduct, ethical guidelines, binding corporate rules, and other kinds of by-laws and technical standards.

Already the sheer volume of privacy-related, regulatory information implies that legal research in the field is not a one-track, narrow-gauge phenomenon. Broad surveys and studies concentrating on details are both common. Typically, the approaches apply what may be called standard methods of legal science. What this means is – as is to be expected – a matter of some disagreement. Without delving into these discussions and matters of general theory of law, mainstream legal science may be characterized in the following way.

- A. Typically, focus is on analyzing what constitutes *valid* law (law in force).
- B. There is a close relationship between practical legal work and legal science. This goes for both problem formulation and methods used.
- C. The core methods of legal science target studies of valid law. Thus, they focus on codified law and are text-oriented and based on intricate rules regarding what constitutes legally acceptable methods of construing and reasoning. A dividing line is usually, and with varying difficulty, upheld between such studies (*lex lata*, law as it is) and studies of what the law should be (*lex ferenda*). From the viewpoint of legal science, the latter

4 The Protection of Personal Privacy. A Map and Analysis. Official Government Reports, SOU 2007:22, two volumes (in Swedish).

kinds of studies are methodologically uncertain. To put it otherwise, they open the door for non-traditional lines of argumentation.

D. The methods of legal science have to do with rule of law and the upholding of a just and democratic society.

Traditional legal science can hardly be described as eager to change its methods and to embrace methodological innovations. It is usually organized according to classical divisions into recognized *fields of law*, a tradition that may cause difficulties for scholars working with problems that presuppose restructuring and alternative patterns. There is also the issue of neighboring disciplines which may be categorized in the following way. Firstly, there are occasional uses of knowledge from other disciplines, e.g., in order to better understand issues in need of legal regulation. Secondly, research projects may be set up so that work with different orientations is conducted in parallel with participants from different disciplines. Thirdly, there are a number of fields where one finds more permanent interaction and integration of views and methods, rather than the occasional interest taken in outside knowledge or simple parallel work. Examples of such fields are criminology, forensic medicine, sociology of law, law and economics, and legal informatics.

As far as law is concerned, privacy protection has been on the agenda for a rather long time. Depending on perspectives and definitions, the history of privacy protection may be seen as quite old. Consider, e.g., the *Lex Sodermanniae* (the Swedish Södermannalagen) from the early 14th century. It contains a chapter on so-called “manhelgd”, which deals with affronts to persons relating to honor, body, and property. Among other things, it contains a provision on wounds inflicted in the victim’s own home (referred to in Section XII as “peace of the home”).

A glance in the rear mirror gives good reasons to distinguish between classical and modern legal privacy research. Admittedly, the distinction is uncertain and riddled with questions. The classical and the modern blend together and there are different ways of separating the two. One useful way of doing so may be to consider *the ripe information society as the modern setting* with an emphasis on phenomena such as global data networks, ubiquitous computing, Semantic Web and affective computing. Such a division immediately calls for refinements and the recognition of a transition phase (an early-modern phase) beginning in the late 19th century with the advent of inventions such as light-weight cameras, mechanical data processing (punched cards), increasingly rapid means of transportation and modern mass media.

The needs for legal research in privacy protection reflect the ongoing changes and their political expressions. They concern many issues of a more or less *narrow* kind, e.g., the protection of children on the Internet or what constitutes

adequate measures to protect the security of personal data. The needs also involve *broad* issues, such as a better understanding of the totality of privacy-relevant regulation, including basic concepts and the overall structure of the regulatory field. The needs foster an interest in both traditional, mainstream type studies (of the *lex lata* kind) and studies with expanded, multidisciplinary perspectives. The latter become particularly important when efforts are made to understand the changing, new situation of privacy protection and, not least, what the future will look like.

A good illustration of work aiming at improved understanding of the changing nature of privacy protection can be found in the ongoing work in the European Union to examine the needs for reforming the Data Protection Directive (95/46/EC, “the Directive”). Among other things, the British Information Commissioner’s Office has commissioned RAND Europe to prepare a study that was published in spring 2009 (Robinson et al. 2009). The study concludes that the Directive has both weaknesses and strengths. For example, the Directive is a reference model for good practice but there is an unclear link between the concept of personal data and real privacy risks. All in all, in the short run, there are needs for improvements with regard to implementation and what is called “effective interpretation”. Not least, the report emphasizes the necessity of making European privacy regulation internationally viable for the future. It clarifies the need to consider the interests of many concerned parties. It outlines a proposed regulatory architecture necessary to secure the regulation in the long term. Some of the suggested reforms are quite far reaching. This can also be said of the conclusion that:

“the success or failure of privacy and data protection is not governed by the text of legislation, but rather by the actions of those called upon to enforce the law. It cannot be stressed enough that supervisory authorities must be given an appropriate level of responsibility for this arrangement to work” (op. cit. p. xiv).

The statement should not be perceived as a degradation of the role of codified law. Instead, it calls attention to the framework that is necessary to make it play its role well. Competent supervisory authorities is one of the elements of such a framework but there are also other ones, sound IT politics and privacy-friendly information system design, e.g.

2.4 Computer and Systems Sciences

Computer professionals have had widely varying concerns for privacy during the different computerization eras of mainframes, personal computers, the

Internet, and ubiquitous computing. Privacy concerns during the era of mainframes addressed a situation where a selected few individuals in large and powerful organizations had access to computer files and database entries regarding citizens and consumers. Personal computers increased the number of people working directly with computers, especially in offices, but the privacy concerns were still related to structured information, primarily concerning working environments and public administration. Networked PCs emerged in the homes as the Internet gained in popularity, which brought computer-mediated communication in to the everyday life of consumers. This broadened the scope of what counts as privacy concerns from a data protection perspective, as the use of automation, information aggregation, and telecommunication technologies increased. This trend has continued with additional elements of media convergence, multiple computing devices (desktop computers, laptops, mobile phones) per person, embodied computing and sensors, which characterize the era of ubiquitous computing (Elliott & Kraemer 2008; Seipel 2008). Privacy concerns are no longer adequately described as emerging in the relations between technology developers, data controllers, and individual data subjects (Bennett & Raab 2006), but require an increased attention to communication and sociotechnical relations between different data subjects.

When socially responsible computer professionals have faced the challenge to design with privacy in mind, they have not only used the techniques of computer science, but also turned towards both legal scholars and social scientists for advice. The main computer science approach can be thought of as making sure that 1) the information sent from person A, and transmitted via computer network technologies to person B, reaches only person B and no one else, and 2) there are no undesired electronic trails of one's own online activity in electronic archives. This approach can also be described as applied data security, or data security where the data is personal information. A number of techniques can be applied to fulfill these goals, including anonymization, encryption, and access control. Design strategies, e.g. with the goal of minimizing the amount of personal information being processed by an information system, also belong here. A lot of this work falls under the umbrella of PETs, which concerns IT measures for the protection of informational privacy by different means, preferably without the loss of functionality.

Computer scientists and legal scholars developed early contacts in the context of data protection, intellectual property rights, computer contracts, and several other fields. Privacy protection emerged in the mid 1960s as part of this common ground. In the 1970s, debates focused on the protection of personal data in large corporate and public administration databases. Note in this context that in the Swedish Data Act of 1973 (the first national legislation of its kind) the object of regulation was not personal data as such but "personal data files". The original version of this law was markedly restrictive and required all

keepers of such files to obtain special permits from the newly created Data Inspection Board. Later developments in Sweden and elsewhere have moved in the direction of more flexible legal views and so called fair information practices as expressed in, e.g., the OECD privacy protection guidelines of 1980 (OECD 1980). The changes of attitudes appear to have stimulated rather than stifled the contacts between computer scientists and legal scholars.

Within computer and systems sciences, these developments have primarily been understood as a confrontation between large organizations and individual consumers. In the light of this perspective, fair information practice principles have been developed in to more detailed privacy *guidelines* (e.g., Langheinrich 2001).

In order to mitigate privacy concerns, computer professionals have typically used best practices emerging from product development: advice regarding the design process. The core ideas of these design guidelines are based on having close collaboration between product developers and users, to consider timing, and to do user-evaluated iterations to get enough user feedback. These approaches to meet user needs have had many names and flavors during different times: socio-technical design (Mumford 2006), participatory design (Bødker, Kensing, & Simonsen 2004), user-centered systems design (Norman & Draper 1986), contextual design (Beyer & Holtzblatt 1997), value-sensitive design (Friedman 1997), and user-driven innovations (Hippel 2005). A distinguishing factor of these privacy-sensitive design approaches is the different ways in which they address privacy. Some treat privacy as a particular user need, some as a value, while yet others address privacy as an integral part of the user experience. However, the challenge of design guidelines is that they are generic, they apply to all design situations, which means that they need a lot of customization for particular privacy design situations. Another challenge is that the generic user-centered design guidelines overlap other privacy guidelines (Iachello & Abowd 2008) and that developers may not necessarily read and follow them.

Computer scientists have, to some degree, also glanced at the social sciences for support – especially when the personal data that requires protection is ill defined, for instance regarding interpersonal communication that is mediated by computer systems. This multidisciplinary research has to a large degree been based on privacy as a boundary regulation and negotiation process (see Section 2.2), where the disclosure of personal information is closely coupled with particular settings and other actors' mediated presence, instead of being specified in advance. Palen & Dourish (2003) refer to regulating the disclosure, identity, and temporal boundaries – for instance by setting the availability status in an instant messaging service. Currently, the discussions concern the effects of changing one's social network status and how that information propagates to unintended audiences, media spaces (Boyle & Greenberg 2005), location-aware

technologies (Krumm 2009) as well as social translucence (Erickson & Kellog 2000) and informed consent online (Friedman, Millet & Felten 2000).

To conclude, in computer science different concerns have been raised under the rubric of privacy during different computerization eras. The main computer science approach to privacy has been to secure transfer of personal data and control electronic trails, for which a number of privacy-enhancing technologies have been developed. The computer science field has been inspired by both law and social sciences, but rarely by both professional fields in the same projects.

3 Summing up – Multidisciplinary Privacy Research

In this section, we examine some aspects of a multidisciplinary framework for privacy studies with particular regard to possible advantages and disadvantages. The reflections in Section 3.1 are general in nature, whereas in Section 3.2, we outline some conclusions that appear to us particularly important for both theoretical and practical reasons.

3.1 Motivating a Multidisciplinary Approach to Privacy Research

Assessing the shape and possible usefulness of multidisciplinary approaches is not trivial. The discussion may be organized according to, e.g., different stages of the research process (ranging from problem awareness to dissemination of results). It may also be a question of trying to identify specific core issues or themes that, for varying reasons (e.g., their complexity), benefit from combinational thinking.

A good understanding of the limits to multidisciplinary endeavors is also of essence – note, e.g., the differences in the overall aims of the three fields under discussion in this paper. Expressed in simple terms, the social sciences try to understand and explain how human beings live together and underscore possible areas of conflict that need special societal attention. The basic goal of law and legal science is to provide mechanisms based on the rule of law for the handling of conflicts and transactions of all kinds in society. Computer and systems sciences again aim at designing and developing information and communication technologies, and in doing so, try to build societally feasible technologies to be used by humans. This means that the primary objectives and the basic motives for addressing privacy-related issues differ in the three fields, and for good reasons. The same can be said for many methodological issues that are intrinsically discipline-specific.

With this note of caution in mind, it should be underlined that a number of risks are associated with disciplinary (i.e. single discipline) privacy research

efforts. In the case of the social sciences, there is a risk of producing theoretical explanations of matters of society with flawed understandings of technology and disregard for different laws in different nation-states. In the case of law, there is a risk of producing defective legal solutions due to insufficient understanding of the interplay between IT and social contexts. Finally, within computer and systems sciences, there is a risk of producing technologies based on erring assumptions about privacy as a social phenomenon, e.g., that people are able to specify their privacy preferences in advance, before their actual experience of a new technology; and technologies that ignore the conflict resolution capabilities that the legal domain can offer.

In Section 2, we described how the three professional fields of the social sciences, law, and computer and systems sciences have developed in a direction where multidisciplinary work seems both natural and motivated. For example, the advent of the networked information society means that many traditional issues of protection of private life and the right to be let alone, i.e. classical privacy law, need to be seen in a new light. The distinction between what belongs to the private sphere and what belongs to the public sphere has become more complicated. But the changes brought about by modernity go deeper. Not only do they add a few aspects to traditional privacy protection problems, they also raise questions regarding broad structural changes and needs for new perspectives. We need new ways of conceiving how the interests of individuals relate to the construction and use of society's information systems. A development in this direction has been going on for some time. With the advent of the Internet and its various innovative applications it appears to be accelerating. Privacy protection is becoming a widespread concern, one may say a sort of scapegoat for a disparate mixture of worries associated with the emergence of a wired society, catering for all kinds of needs and maintaining and using vast volumes of information about people and things. These worries have to do both with the situation of individuals and with societal concerns (e.g., administrative efficiency, democracy, and markets).

Privacy protection issues take on new shapes and significance in the networked information society. This development implies that privacy protection as a field of law has expanded and grown in social significance. It has also become a sort of meeting place for many concerns and interests having to do with IT and having privacy protection as a common denominator. Research in the field needs to go beyond traditional studies of valid law. Cooperation with other disciplines leads to a better understanding of basic concepts and frameworks (such as social networks) and of the ways in which law can assist in creating information systems that are not only acceptable but helpful to the citizens.

Similarly, recent social theories stressing the importance and interplay of different sociotechnical systems in the study of privacy help to articulate and

associate findings from different disciplines. Instead of focusing mainly on the relationship between institutions and humans, special emphasis is placed on the larger networks of which they are parts. Within these theories the range of important actors in the study of how social life is constituted is multiplied – the research methods involve looking at empirical connections between humans, material technologies, social conventions, and legal frameworks. Here, privacy is seen neither in a techno-deterministic way, nor with romantic ideals of perfect privacy in a golden age of long ago, but as a struggle to find a balanced description through which these two perspectives can be seen as co-constituting each other. Privacy and social life, humans and material technologies, politics and legal concerns all interact with each other through shifting relations, and without any one of them being the final (the *master*) explanation for the others – silenced actors, social divisions and the partiality of any one viewpoint are all acknowledged.

The sharing of *issues* (e.g., the public vs. the private spheres, informed consent, location-aware technologies), *approaches* (e.g., privacy as a value, *lex ferenda*, best design practices), *factual descriptions* (e.g., user preferences, ways of communication, technical developments), etc., that characterize multidisciplinary activities should not be confused with abandoning or replacing the basic aims and responsibilities that each of the three fields considers to be at its heart. Rather, the rationale of multidisciplinary research is that, at its best, it contributes to creating shortcuts to insights, which are difficult or not possible to come by when attention is limited to viewpoints, perceptions, traditions, and ways of questioning and reasoning about privacy within one's own field of expertise. This goes both for identifying what understandings of privacy are relevant in a particular context and for the formulation of the associated research questions.

The interest in developing the research methods of each participating field should also be mentioned. This self-interest point of view is certainly important and can be seen as a sort of cross-fertilization. Again using law as an example, the multidisciplinary engagement can be of value for increasing the quality of studies of the *lex ferenda* type (law as it ought to be).

Last but not least, multidisciplinary approaches can increase the usefulness of invested research efforts in that the results become parts of mixed knowledge pools that are shared by experts from different fields. For this to occur it is essential that attention is paid to the barriers that usually keep fields of research apart, different terminologies, different priorities, different research styles, just to mention a few.

3.2 The PRIMA Approach to Multidisciplinary Privacy Research

The PRIMA project studies the ways in which penetration, development and use of IT (e.g., ubiquitous interaction, augmented reality, self-made media) have affected, affect and possibly will affect different stakeholders in sociotechnical settings giving rise to privacy protection issues (see, e.g., Bylund, Höök & Pommeranz 2008; Lehmuskallio, Tamminen & Johnson 2009; Lehmuskallio 2009; Neuvonen 2009; Rähä & Ovaska 2009). Not least, our interest concerns how privacy is managed and how conflicts that arise can be coped with by actors themselves, solved by regulation of different kinds (e.g., policies, binding corporate rules, and statutes) or can be handled by various technical means. Given this framework, we also attempt to gain a better understanding of multidisciplinary work with regard to its potentials and deficiencies as well as how it can be organized.

One finding, which may seem so trivial that it is easily overlooked, has to do with the usefulness of creating an environment where researchers with different theoretical backgrounds actually work together and strive to learn about the other parties' perceptions of privacy and privacy protection. Such working modes take (extra) time, they can cause irritation and be uncomfortable. Basically, they presuppose that every participant ceases to aspire to the role of the super expert and accepts that his or her own knowledge is certainly not complete. Looking at the issue from a practical point of view, many projects where advice is sought from outside experts fail because of misunderstandings, different language use, and too little time to develop a shared framework for the work.

As pointed out above, multidisciplinary is not always an advantage. It is necessary to distinguish particular issues or areas where gains are likely to occur. The following list summarizes the PRIMA experience.

The formulation of *ultimate* goals of privacy protection schemes profit by multidisciplinary approaches. A good grasp of where we are heading can serve as a pruning instrument for regulatory efforts and a common point of reference for the participating fields of research. Given the underlying differences between the individual research fields, these goals cannot be spelled out in too much detail, assuming specific epistemologies and ontologies. The key to successful multidisciplinary work is to plan the research efforts so that results from individual disciplines feed into each other, thus effectively working together to achieve the top-level goals.

A neighboring concern has to do with the design of society's *informational infrastructure*. This is the environment where today's main privacy protection

issues are located. It is a complex and partly new world where basic legal moorings are often missing or have taken on new forms and meaning.

The putting together of toolboxes containing standard appliances for dealing with privacy problems has been pointed out as essential. The PRIMA project shares this view and acknowledges the value of familiarizing researchers with the needs and how they can be met in different contexts. Not least, areas such as *privacy by design* and *privacy enhancing technologies* can be fitted into this discussion. It is to be noted that the toolbox strategy supports efforts to make law more proactive. Briefly put, it leads to an improved understanding of how particular legal measures (such as informed consent) can be plugged into standardized technical tools as a means of implementation. When and if such schemes work they speed up the whole process of legal regulation and contribute to the foreseeability that is such an important element of the rule of law. In other words, the toolbox strategy helps actors (such as the administrators of social networks) understand their responsibilities and facilitates their efforts to put together and operate privacy-friendly systems.

References

- Altman, I. 1975. *The Environment and Social Behavior. Privacy - Personal Space - Territory - Crowding*. Monterey: Brooks-Cole Publishing Company.
- Altman, I. 1977. *Privacy Regulation: Culturally Universal or Culturally Specific?* *Journal of Social Issues* 33, 3: 66-84.
- Appadurai, A. 1996. *Modernity at Large. Cultural Dimensions of Globalization*. Minneapolis: University of Minnesota Press.
- Arendt, H. 1958. *The human condition*. Chicago: The University of Chicago Press.
- Bennett, C. J., and Raab, C. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA, USA: MIT Press.
- Beyer, H, and Holtzblatt, K.. 1997. *Contextual Design: A Customer-Centered Approach to Systems Designs*. 1st ed. Morgan Kaufmann, September 15.
- Blumer, H. 1969. *Symbolic Interactionism. Perspective and Method*. Berkeley: University of California Press.
- Bødker, K., Kensing, F., and Simonsen, J. 2004. *Participatory IT Design: Designing for Business and Workplace Realities*. The MIT Press, October 1.

- Boyle, M., and Greenberg, S. 2005. *The language of privacy: Learning from video media space analysis and design*. ACM Transactions on Computer-Human Interaction (TOCHI). 12, no. 2: 328-370.
- Bowker, G.C. and Star, S.L. 1999. *Sorting things out: classification and its consequences*. Cambridge, MA: MIT Press.
- Bygrave, L.A. 2002. *Data Protection Law. Approaching Its Rationale, Logic and Limits*. The Kluwer Law International.
- Bylund, M., Höök, K., and Pommeranz, A. 2008. *Pieces of identity*. In *Proceedings of the 5th Nordic Conference on Human-Computer interaction: Building Bridges* (Lund, Sweden, October 20 - 22, 2008). NordiCHI '08, vol. 358. ACM, New York, NY, 427-430.
- Callon, M. 1986. *Elements of a sociology of translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay*. In John Law (Ed.), *Power, Action and Belief: A New Sociology of Knowledge?* London, Routledge: 196-233.
- Clarke, A.E. 2005. *Situational Analysis - Grounded Theory After the Postmodern Turn*. Thousand Oaks: Sage.
- Clarke, A.E., & Star, S.L. 2003. *Symbolic Interactionist Science, Technology, Information and Biomedicine Studies*. Pp. 539-574 in *Handbook of Symbolic Interaction*, edited by L. T. Reynolds & N. J. Herman. Walnut Creek, CA: Alta Mira Press.
- Craddock, A.E. 1997. *The measurement of privacy preferences within marital relationships: The Relationship Privacy Preference Scale*. *American Journal of Family Therapy* 25, 1: 47-53.
- Crossley, N., ed. 2004. *After Habermas. New Perspectives on the Public Sphere*. Oxford et. al: Blackwell.
- Engeström, Y., Miettinen, R. and Punamäki, R.L. ed. 1999. *Perspectives on activity theory*. Cambridge, New York: Cambridge University Press, 1999.
- Elliott, M.S., and Kraemer, K.L. 2008. *Computerization Movements and Technology Diffusion: From Mainframes to Ubiquitous Computing*. Information Today, Inc., February 26.
- Erickson, T. and Kellogg, W. A. 2000. *Social translucence: an approach to designing systems that support social processes*. ACM Trans. Comput.-Hum. Interact. 7, 1 (Mar. 2000), 59-83.
- Etzioni, A. 1999. *The Limits of Privacy*. New York: Basic Books.
- Etzioni, A. 2004. *The Common Good*. Polity Press.

- Fraser, N. 1993. Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy. In: Calhoun, Craig (Ed.), *Habermas and the Public Sphere*. Cambridge, MA et. al, MIT Press. 109-142.
- Friedman, B. 1997. *Human Values and the Design of Computer Technology*. 1st ed. Center for the Study of Language and Information.
- Friedman, B., Millett, L., & Felten, Ed. (2000). *Informed consent online: A conceptual model and design principles*. (UW CSE Technical Report 00-12-02.) Seattle, WA: University of Washington, Department of Computer Science and Engineering.
- Habermas, J. 1962. *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Neuwied am Rhein, Berlin: Luchterhand.
- Hippel, E. von. 2005. *Democratizing Innovation*. The MIT Press.
- Iachello, G. and Abowd, G.D. 2008. *From privacy methods to a privacy toolbox: Evaluation shows that heuristics are complementary*. ACM Trans. Comput.-Hum. Interact. 15, no. 2: 1-30.
- Iachello, G. and Hong, J. 2007. *End-user privacy in human-computer interaction*. Found. Trends Hum.-Comput. Interact. 1, 1
- Kaptelinin, V. and Nardi, B.A. 2006. *Acting with technology: activity theory and interaction design*. Cambridge, MA et. al: MIT Press.
- Krumm, J. 2009. *A survey of computational location privacy*. Personal Ubiquitous Comput. 13, 6 (Aug. 2009), 391-399.
- Kumaraguru, P. and Cranor, L.F. 2005. *Privacy Indexes: A Survey of Westin's Studies*. Technical Report CMU-ISRI-05-138. Institute for Software Research International, School of Computer Science, Carnegie Mellon University.
- Langheinrich, M. 2001. *Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems*. In Proceedings of the 3rd international conference on Ubiquitous Computing, 273-291. Atlanta, Georgia, USA: Springer-Verlag.
- Latour, B. 1987. *Science In Action: How to Follow Scientists and Engineers Through Society*. Cambridge Mass.: Harvard University Press.
- Law, J. and Mol, A. eds. 2002. *Complexities: Social Studies of Knowledge Practices*. Durham, NC: Duke University Press.
- Lehmuskallio, A., Tamminen, S. and Johnson, M. 2009. *Managing Privacy on Social Network Sites*. In: Medienamateure. Wie verändern Laien unsere visuelle Kultur?, Universität Siegen 5.-7.6.2008, www.medienamateure.de/pdfs/LehmuskalliouaManaging.pdf.

- Lehmuskallio, A. 2009. *A photo is not an extension of me, it's plain surface. – Views of users of a Web 2.0 photo-sharing site on photos and privacy.* SPIEL: Siegener Periodicum zur Internationalen Empirischen Literaturwissenschaft, Phenomena of Web 2.0 as agents of cultural change, in press.
- Locke, J. 1960. *Two treatises of government.* Cambridge: Cambridge University Press.
- Margulis, S.T. 2003. *On the Status and Contribution of Westin's and Altman's Theories of Privacy.* Journal of Social Issues 59, 2: 411-429.
- Marshall, N.J. 1974. *Dimensions of Privacy Preferences.* Multivariate Behavior Research 9, 3: 255-272.
- Mumford, E. 2006. *The story of socio-technical design: reflections on its successes, failures and potential.* Information Systems Journal 16, no. 4 (October): 317-342. doi:10.1111/j.1365-2575.2006.00221.x.
- Neuvonen, T. 2009. *Practices of Privacy: A User Perspective on Online Picture Sharing,* Master's thesis, Department of Sociology, University of Helsinki.
- Newell, P. 1998. *A cross-cultural comparison of privacy definitions and functions: a systems approach.* Journal of Environmental Psychology 18, 357-371.
- Norman, D.A., and Draper, S.W. 1986. *User Centered System Design: New Perspectives on Human-computer Interaction.* 1st ed. CRC, January 1.
- OECD. 1980. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
- Palen, L. and Dourish, P. 2003. *Unpacking "privacy" for a networked world.* In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Ft. Lauderdale, Florida, USA, April 05 - 10, 2003). CHI '03. ACM, New York, NY, 129-136.
- Pedersen, D.M. 1996. *A factorial comparison of privacy questionnaires.* Social Behavior and Personality 24, 3: 249-262.
- Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure.* Albany, NY: State University of New York Press.
- Regan, P. 1995. *Legislating Privacy. Technology, Social Values and Public Policy.* Chapel Hill: University of North Carolina Press.

- Robinson, N., Graux, H., Botterman, M., Valeri, L. 2009. *Review of the European Data Protection Directive*, RAND Europe Technical Report (TR710). Available at http://www.rand.org/pubs/technical_reports/TR710/
- Räihä, K. and Ovaska, S. 2009. Faces of Privacy: Effect of Culture and Context. In *Proceedings of the 12th IFIP TC 13 international Conference on Human-Computer interaction: Part I* (Uppsala, Sweden, August 24 - 28, 2009). T. Gross, J. Gulliksen, P. Kotzé, L. Oestreicher, P. Palanque, R. O. Prates, and M. Winckler, Eds. Lecture Notes In Computer Science, vol. 5726. Springer-Verlag, Berlin, Heidelberg, 700-703.
- Rössler, B. 2005. *The value of privacy*. Cambridge, UK ; Malden, MA.: Polity.
- Seipel, P. 2002. *Law and ICT. A Whole and its Parts*. In: Law and Information Technology. Swedish Views. Ed. P. Seipel. Swedish Government Official Report SOU 2002:112.
- Seipel, P. 2008. *Alone no More*. In: Festskrift till Marianne Levin. Ed:s A.B. Engelbrekt. Stockholm: Norstedts Juridik.
- Seipel, P. 2009 *Privacy in the Making* Workshop 2008. Notes and comments. Available at <http://www.juridicum.su.se/iri/e08/>
- Sennett, R. 1977. *The fall of public man*. Cambridge: Cambridge University Press.
- Warren, S. D. and Brandeis, L. D. 1890. *The right to privacy*. Harvard Law Review 4(5):193-220.
- Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.
- Westin, Alan F. 2003. *Social and Political Dimensions of Privacy*. Journal of Social Issues 59, 2: 431-453.