Report from Dagstuhl Seminar 14052

Ethics in Data Sharing

Edited by

Julie Cohen[1], Sven Dietrich[2], Aiko Pras[3], Lenore D. Zuck[4], and Mireille Hildebrand[5]

1 **Georgetown University – Washington, DC, US,** jec@law.georgetown.edu
2 **Stevens Institute of Technology, Hoboken, NJ, US,** spock@cs.stevens.edu
3 **University of Twente, NL,** a.pras@utwente.nl
4 **University of Illinois at Chicago – Chicago, IL, US,** lenore@cs.uic.edu
5 **Vrije Universiteit Brussel – Brussels, BE**

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 14052 "Ethics in Data Sharing". The seminar brought together computer scientists, an ethicist and legal scholars to discuss the topic of "ethics in data sharing."

Seminar January 26–31, 2014 – http://www.dagstuhl.de/14052
1998 ACM Subject Classification K.4.1 Public Policy Issues, K.6.5 Security and Protection, K.7.4 Professional Ethics
Keywords and phrases Ethics, Data Sharing Practices, Data Dissemination, Ethics across borders, Anonymization, Sanitization
Digital Object Identifier 10.4230/DagRep.4.1.170

1 Executive Summary

Julie Cohen
Sven Dietrich
Aiko Pras
Lenore D. Zuck
Mireille Hildebrandt

ACM's ethical guidelines (as well as IEEE's) are almost two decades old. The most relevant points to data sharing it makes are "Avoid harm to others" and "Respect the privacy of others." The consequences of not complying with the code are "Treat violations of this code as inconsistent with membership in the ACM" while "Adherence of professionals to a code of ethics is largely a voluntary matter."

In fact, in the current legal system, ethical behavior "doesn't pay." Such guidelines are insufficient for the numerous professionals working for corporations where privacy policies are dictated more by a company than by its employees. Nowadays, we have little control who receives our Personally Identifiable Information (PII), what PII they receive, where collected PII is transferred to, and what is the source of (mis?)information others have on us. This is especially alarming with the rapid progress of data mining, the constant discovery of flaws in data anonymization/sanitization techniques, and the vast amount of electronic data that exists. It is beyond the ability of a layperson to understand the privacy policy of organizations and their consequences on the individual.

Ethics in Data Sharing, *Dagstuhl Reports*, Vol. 4, Issue 1, pp. 170–183
Editors: Julie Cohen, Sven Dietrich, Aiko Pras, Lenore D. Zuck, and Mireille Hildebrand
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The situation is even more serious when data is shared and disseminated among different countries that naturally have different ethical codes and policies for dealing with privacy issues concerning data sharing. Data transfer has no borders, hence, neither does data sharing, which renders ethical data sharing all the more challenging.

However, the recent EU proposals to update the legal framework of the Fair Information Principles, precisely with an eye to the emergence of hyperconnectivity and ubiquitous data analytics, has introduced the notion of Data Protection by Design. This may provide strong incentives to introduce purpose binding, informed consent, minimal disclosure and profile transparency into the design of the relevant computing systems.

The seminar brought in researchers from all disciplines that involve data sharing across borders with ethical implications. The main focus was on Computer System Security data, with consideration for Electronic Medical Records. We derived a basic model for data sharing, and came up with some suggestions of code of ethics for computer professionals (including researchers) that will elaborate on existing codes in terms of data sharing.

2 Table of Contents

3 Overview of Talks

3.1 Privacy, Surveillance, and Ethics

Julie E. Cohen (Georgetown University – Washington, DC, US)

Main reference Julie E. Cohen, "What Privacy Is For," Harvard Law Review, 126.7 (May 2013):1904–1933.
URL http://harvardlawreview.org/2013/05/what-privacy-is-for/
URL http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf

The ways that privacy and surveillance are understood make the task of formulating ethical guidelines for data sharing a complex one.

Privacy: Particularly in the U.S., but also to an extent in Europe, legal and political discourse conceptualizes privacy as a form of protection for the liberal self. So understood, however, privacy's principal function is defensive and reactionary. It preserves negative space around individuals who are already autonomous and fully formed, providing shelter from the pressures of societal and technological change. In fact, the liberal self who is the subject of privacy theory and privacy policymaking does not exist. The selves who are the real subjects of privacy law- and policy-making are socially constructed, emerging gradually within situated cultures and networks of relationships. Properly understood, privacy's function is dynamic. It shelters emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. Privacy exists in the gaps within frameworks of social control, and this makes it an indispensable structural feature of liberal democratic political systems. Because privacy shelters play, experimentation, and critical reflection, it is also foundational to the capacity for innovation.

Surveillance: The understanding of surveillance and its relationship to government is changing. Traditional discourses about surveillance have emphasized discipline and control. Today, crowd-sourcing and gamification have become important strategies for collection and processing of personal information, and legal strategies for open access and open innovation also have emerged as important drivers. Many development projects that rely on personal information are framed as open access projects, and seek to exploit and profit from the intellectual cachet that rhetorics of openness can confer. Meanwhile, participants in legal and policy discourses about privacy and data processing work to position privacy and innovation as opposites, and to align data processing with the exercise of economic and innovative liberty. The resulting template for surveillance is light and politically nimble. Commentators have long noted the existence of a surveillance-industrial complex: a symbiotic relationship between state surveillance and private-sector producers of surveillance technologies. The emerging surveillance-innovation complex represents a new phase of this symbiosis, one that casts surveillance in an unambiguously progressive light and paints it as a modality of economic growth. At the same time, the rhetorics of openness and innovation work to keep the regulatory state at arms length.

Translating Critique into Practice: Privacy is a function of structure (built environment, networked environment, etc.) and practice. Both effective privacy regulation and effective design for privacy must mind the gaps. Design practices favoring seamless interoperability and scalability probably need to be rethought from the ground up.

3.2 People can't control access to their data

Jürgen Schönwälder (Jacobs Universität – Bremen, DE)

A couple of years ago, we started getting interested in the question how far it is possible to identify users from network flow traces. We believe this is actually feasible for a large set of diverse users (although clear bounds on the error rate still need to be determined). But of course, all this raises concerns whether this research is ethical to do. We argued that other organizations are likely doing this work behind closed walls and we prefer to do it in an open fashion and to write about it in order to raise awareness. Others argued that doing this kind of research (a) violates current laws and (b) research results enables even more privacy infractions. So what is the right thing to do? Should researchers actively develop techniques to break privacy? Is this like in cryptology where you have people specializing into cryptography and cryptanalysis?

Concerning privacy, I believe (and did so years before PRISM) that we have lost privacy and that in particular normal people have not even a slight idea of what is possible with today's networked systems. If we start from the premise that ordinary people can't control their privacy anymore, will we see new businesses offering privacy services to ordinary people (privacy as a service)? Is there any chance that laws will protect privacy in a globalized networked world? What is the privacy incident that is big enough for the public sensitivity to privacy related questions to change?

People can't control access to their data. Even if they try, today's systems make it easy to correlate data and to identify individuals. What are the solutions? (a) Produce so much data that correlation systems fail? (b) Design special systems like e.g., Tor to hide communication? (c) Have 3rd parties involved that manage personal data? (d) Give up, we have lost privacy, it won't come back...

3.3 Sound experimentation for computer security

Darren Shou (Symantec Research Labs – Culver City, CA, US)

In 2010 we created a platform to enable sound experimentation for computer security. We hoped that we could tip the balance of the security arms race and unlock strategic insights. In 2011 we tried to address ethical considerations to share and of sharing data. Now I am concerned with big data and the impact on the expectation of privacy, second chances, and a new social network economy.

Important Topics:

- What are our options for sharing security research data (or other data) that enable multi-national enterprises and what might be the unintended consequences?
- What are the long term cultural and ethical considerations enabled by big data, that is, what if there is no privacy?
- How would a new economy such as the current multi-level business model evolve to handle privacy issues (i.e. how can a company that provides a free service to users by selling their data to advertisers evolve?)
- Should users control the flow of their information?

3.4 Ethics in Networking Research

Burkhard Stiller (Universität Zürich, CH)

The talk on “Ethics in Networking Research”is based on 2 definitions, 4 main observations, and follows with 3 open and 6 even wider open issues, which determine at least a few lines of inter-disciplinary research challenges.

Firstly, the definition of ethics as a system of moral principles, guided by a set of rules of conduct recognized in respect to a particular class of human actions or a partial group, culture, education, location leads to the moral principles as of an individual. In turn, ethics guide our life and it remains a very relative metric across borders. Note that there is a clear difference between ethics and legal statutes, since not all ethics is coded into laws and they may vary very much according country-specific perceptions. And, an evolution of ethics, laws, and rules is happening on a daily basis.

Secondly, determining data as raw data, combined with context, meta, and additional data, defines the basis for the process of data sharing, which enables the analysis of real life happenings of networking. However, besides the pure networking data, multiple application-related data (such as health data or banking data) incur an ethics dimension, especially in terms of knowing about their details, their possible use, and their exploitation.

Consequently, neither complete nor in full, but driven by major networking views, 3 observation tend to occur. (1) The handling, analysis, usage, interpretation, and relevance simply changes upon technology changes from hard drives, to clusters, clouds, and tomorrows extraterrestrial storage locations. (2) The main areas of conflict cover the (a) researcher’s view, (b) the operator’s view, and (c) the personal (user’s) view, each of which with valid targets on their own, such as (a) in search of the real reason and knowledge gains, (b) improving reliability, performance, compliance, . . . , and (c) respecting privacy and providing access to functionality demanded for. Independent of each of those categories, all stakeholders are formally bound by legal and regulative constraints, in which ethics are not part of explicitly (at least not in many cases), however, in which many ethical dimensions play a role in, sometimes formalized by ethical boards or discussion fora. (3) Finally, the handling, analysis, and usage of data is the key for networking research, which should be based on a (public) study plan and a respective protocol. This has developed over time to a certain standards level in the medical discipline, however, “standardization” there has been acknowledged only to a certain level. In any case, in networking research the raw data needs to be shared, including the meta data, especially to ensure reproducability and proof of findings related to those data. Such work may be based on best practices (which change often, too). Since such networking data contains personal data, the violation of privacy always happens, either in a foreseen or in an unforeseen manner. As one very simple example in that dimension utilities’ usage and its measurements serves as an optimization approach for personal behaviors (privacy aspect) and its reveal to the utility provider, who can access detailed, time-based usage information of a single house-hold.

Due to these very few observation taken – there are hundreds other ones not listed explicitly – the 3 challenges of next steps in research, public policy, and regulations driven are addressing the basics:

1. What are the impact factors on ethics applied to networking research, especially on data and information? Does this list include legality, regulation, usability, reproducability, practicability, responsibility, commercialization, sustainability, auditability, . . .

2. What are the mandatory demands derived from those for an ethical networking research?
3. Is there any general way to provide practical guidelines besides use cases only?

Even wider open issues in a more case-specific perspective include the following 6 ones:

1. Can networking research achieve the same level of best practices in study protocols, as e.g., in the medical field? Do we want to see that happening anyway?
2. How to deal with inter-domain, multi-domain scenarios, aspects, usages, analysis, and violations as well as court cases? While being "locally" enforceable, the remote case may not provide any "access" to any enforcement technology (if it even exists), a legal body may not be attainable, a foreign court may consider itself as being not responsible, and once data leaked, they leaked.
3. Even is the use of specific data is unethical in its core form, how to prevent the misuse of those data by third parties? Is an NDA sufficient, how to enforce authorized accesses only, how to handle the case of whistleblowers, is there a guarantee on data deletion, is there a chance to ensure the handling of data only according to purpose, self-destroying otherwise?
4. Is the use of methods, which are unethical and sometimes even illegal in themselves, but which attackers use, ethical, especially to prevent harm and disasters? In such a case legal aspects have to be discussed on a separate track, which needs to include country-specific views and intelligence agencies, too.
5. How to act as a personal individual, as a researcher? What about the person, the employee, the government? How to deal with or encourage loyalties and whistleblowing?
6. If a technical experiments is illegal, it may be still relevant ethically, is that a path to promote? For example the African Spring uproars made changes happen (to the good or the bad – that's not discussed here), which were based on the violation of law in force.

Thus, concluding, the dimensions at which ethics affect networking research are larger than someone initially may assume, but they do show at the same time that flexible borders exist and that some of those or neither clear nor viable for that many technologies and applications in use as of today.

3.5 Unintended Consequences of Data Sharing Laws and Rules

Sam Weber (Software Engineering Institute – Arlington, VA, US)

Sharing of cybersecurity and health care data involves ethical and legal issues, as well as concerns about the utility of said data. My talk will focus on the unintended consequences of well-meaning privacy policies and regulations. In particular, I will discuss three real-life examples where seemingly sensible regulations have negative consequences.

3.6 Packets don't know about ethics

Roland van Rijswijk-Deij (Radboud University Nijmegen, NL)

Main reference Blog article on Dagstuhl Seminar "Ethics in Data Sharing"
URL https://blog.surfnet.nl/?p=3174

Being a researcher and working at a National Research and Education Network (NREN) is like permanently living in a cookie jar brimming with exquisite chocolate chip cookies. There is unlimited access to a sea of big data that can be used for research on networks. Also, because of their not-for-profit and academic nature, NRENs are inclined to share this big data not only within their organisations but also with academic groups with which they partner to perform research on networks.

While having access to all this data is ideal for research, it comes with a significant ethical problem. Most of the data used for research on networks is highly privacy sensitive; it can be traced back to individual users in many cases and can be used to build extensive profiles of these users. Some of the data has no direct content, but is in stead considered "meta data" (for example what we call flow data, information about who communicates with whom at what time in with which protocol). But even based on this meta data, highly invasive personal profiles can be constructed that predict traits of an individual users with a high probability. An example of this is research performed by Katikulapudi et al. [1], in which the authors analysed the Internet use of a group of students based on network flow data. Prior to monitoring Internet use, study participants completed a Center for Epidemiologic Studies Depression (CES-D) depression scale survey. Katikulapudi et al. then show a correlation between certain characteristics of the study participants' Internet use and a high score for depression on the CES-D survey. This is only one example of how bulk analysis of Internet use patterns can reveal highly private information about individuals.

What is worrying is that the kind of data that researchers who perform research on networks use allow these kinds of analyses on the behaviour of individual users, even if the goal of their research probably is not to do so (but rather, for instance, to learn something about the behaviour of certain network services in the face of a severe denial-of-service attack).

Note: I have published an extensive report about my participation in this seminar on SURFnet's innovation blog. The URL for this report is http://blog.surfnet.nl/?p=3174.

References

1 Raghavendra Katikalapudi, Sriram Chellappan, Frances Montgomery, Donald Wunsch, and Karl Lutzen. Associating Internet Usage with Depressive Behavior Among College Students. *IEEE Technology and Society Magazine*, 31(4):73–80, 2012.

3.7 Advancing NREN to Researcher Data Sharing: following up on Dagstuhl

Roland van Rijswijk-Deij (Radboud University Nijmegen, NL)

Main reference Blog article on Dagstuhl Seminar "Ethics in Data Sharing"
URL https://blog.surfnet.nl/?p=3174

Introduction

As a follow-up to the Dagstuhl Seminar on Ethics in Data Sharing, SURFnet has started a project to professionalise the way it shares data with researchers both within as well as outside of it's constituency. This abstract briefly describes the steps we are taking to follow up on the seminar.

Current practice

To understand our starting point, the current practice for sharing data between SURFnet, as an NREN, and researchers is summarised below.

The current practice is that we share data under a non-disclosure agreement that covers:

- What data is shared
- For what purpose the data may be used
- Who has access to the data
- How long the data may be stored and when it must be destroyed
- Conditions of publication (e.g. references to individual IP addresses must be anonymised)

The collective participants of the Dagstuhl seminar agreed that this was a very prudent practice, but there are some downsides to this approach. First of all, current practice is that we usually have a personal relationship with the researchers that forms a foundation of trust that if we share data it is treated ethically and with respect. Good as this may be, it gives us little foundation for sharing data with researchers we do not know personally. And from a scientific perspective, it would be better if some of the data we share would also be made available to other researchers so they can reproduce research.

Following up on Dagstuhl

To follow up on the fruitful discussions at the Dagstuhl Seminar on Ethics in Data Sharing, SURFnet has initiated a project in which some of the attendees to the Dagstuhl Seminar participate. The goal of this project is to come up with a comprehensive policy for data sharing between SURFnet as an NREN and research within as well as outside of its constituency. The policy must cover both the ethics side (how to review research proposals, who will review proposals on both sides of the data sharing agreement, training of reviewers, ...) as well as the legal side (impact of privacy law, contracts, ...).

A first project meeting took place on March 25th 2014 with participants from SURFnet, the research community, ethics and law. The outcome of this meeting is that work will start on a number of action items:

- An analysis of applicable law (focusing on EU and Dutch law)
- An outline for a booklet on ethics for researchers as well as proposal reviewers (review board members)
- A proposal for training of researchers and review board members
- Case studies of past and possible future data sharing requests

A follow-up meeting where the first results of these actions will be discussed is scheduled for June 19th 2014.

We believe that the outcome of this project will have broader applicability than just within SURFnet's constituency. We plan to reach out to other European NRENs and will also sollicit input from the security and network industry.

3.8 To use or not to use:When and for what should researchers use data obtained from social networking sites.

Aimee van Wynsberghe (University of Twente, NL)

Joint work of van Wynsberghe, Aimee; Been, Henry; van Keulen, Maurice
Main reference A. van Wynsberghe, H. Been, M. van Keulen, "To use or not to use: guidelines for researchers using data from online social networking sites".
URL http://responsible-innovation.org.uk/torrii/resource-detail/1471

In the current age of abundant information sharing and gathering, social networking sites (SNSs) are now thought of as incredible resources for collecting data on individuals. To date, such data is collected in a variety of ways (e.g. passively or aggressively), by a variety of researchers (e.g. academic, industry, governmental) for a variety of purposes (e.g. detecting fraudulent behaviors, detecting consumer patterns, studying user patterns). Given this range in collection methods and uses of the data, the question of importance for ethicists, researchers and citizens alike has to do with when and for what can such data be used? In other words, what are the ethics of using data obtained from social networking sites for research purposes? Even when researchers make attempts at protecting the privacy of subjects, things can go wrong, e.g. Facebook's Tastes, ties and Time project and the release of data in 2008. Given the lack of best practices in terms of applying ethics to this field of research, this presentation aims to present a variety of issues related to the use of data obtained through SNSs along with guidelines or points for debate, regarding how to construct a best practice for ethical research. This guideline is created using suggestions from the current literature as well as first-hand experience as an ethics adviser for a research institute dealing specifically with the research and design of ICT systems.

3.9 Ethical considerations of using information obtained from online file sharing sites the case of the PirateBay.

Aimee van Wynsberghe (University of Twente, NL)

Joint work of van Wynsberghe, Aimee; van der Ham, Jeroen
Main reference A. van Wynsberghe, J. van der Ham, Jeroen, "Ethical considerations of using information obtained from online file sharing sites – the case of the PirateBay," in Proc. of ETHICOMP 2014, to appear.

Since the creation of Napster back in the late 1990s for the sharing and distribution of MP3 files across the Internet, the entertainment industry has struggled to deal with the regulation of information sharing at large. From an ethics perspective, the practice of file sharing over the internet presents an interesting value conflict between the protection of intellectual property on the one hand (Von Lohmann, 2003), and fairness on the other (DeVoss and

Porter, 2006). On the one hand, the entertainment industry wishes to uphold their exclusive copyrights to the content, to maintain their business model and their distribution methods. On the other hand, users are demanding easy access to music, television and movie files, and will resort to file-sharing when it is not available at a fair price, or at all. With this in mind, the aim of this paper is to investigate the ethical issues arising from the collection of data from an online sharing site. Most notably the website known as ThePirateBay (TPB), founded in Sweden in 2003, facilitates peer-to-peer file-sharing of movies, music, television programs and more. In different countries the entertainment-industry lobbying organizations are taking different approaches to combat this issue. For a variety of European countries, access to TPB is blocked but users are finding ways around this. In the Netherlands, the entertainment industry has successfully won a court case against TPB forcing them to block users from the Netherlands. The website, however, has not recognized the ruling and has not taken action to block any users in the Netherlands from accessing the site. As a next step the Internet service providers (ISPs) have been taken to court to force them to block access to TPB website. This situation has provided a unique opportunity to study the effects of a website blockade on the file sharing behavior of consumers. It seemed common knowledge for Dutch Internet users that there were ways around the blockade, but the net effect was never measured objectively. A study to this effect is relevant for the Internet Society Netherlands Transparency Working Group, but also for both sides in the court cases (the entertainment industry as well as the Internet providers). To that end, van der Ham et al. (2012) began to measure whether preventing access to these sources of links (i.e. ThePirateBay) has an impact on file sharing behavior of users in the Netherlands. To accomplish this goal the researchers created a tool to measure file sharing activity resulting from links shared through TPB website. The measurement tool takes advantage of the fact that file sharing users use a peer-to-peer sharing mechanism, where part of this mechanism is 'gossiping' IP addresses of other users. This uniquely identifies file sharers and impacts the privacy of these users. Thus, aside from the value conflict when one considers the use of file sharing sites like TPB there exists an additional value conflict when one considers the development of a tool to collect and use the data obtained from such a site. Only after developing this tool and performing the measurements did the researchers realize an ethical analysis of this approach may have been in order. With this, they sought the advice of an ethics adviser (van Wynsberghe). The aim of this paper is two-fold:

1. to conduct an ethical analysis on the collection and use of data obtained through online file sharing sites, and
2. to explore the role and utility of ad-hoc ethics advice.

Both goals use the example of this TPB research as a case study for analysis. For the former, the data collection described here is closely in line with the collection of data from online social networking sites. Thus, to address the ethical issues we will use the framework developed by van Wynsberghe and Been (2013) for the collection of data from online social networking sites. This framework entails an analysis of decision variables and choices of the researcher rather than a study of the ethical intentions (Chen, Y-C et al. 2008) or decision making choices of file sharers (Shang, R-A, 2008). As such the framework is concerned with: the context of use and the privacy concerns for this context; the type and method of data collection; the intended use of information and the amount of information collected; and, analysis of values (e.g. to make explicit and scrutinize designer values). Questions pertaining to the use of the information collected in this research revealed that the stakeholders have a vested interest in proving the effectiveness or non-effectiveness of a file sharing block. This information concerning (non-)effectiveness can be used for different purposes depending on the stakeholder. For instance, the entertainment industry can use the measurements to identify file sharers in support of their copyright infringement case. Alternatively, the Internet Society Netherlands is an organization that sees the censoring of Internet traffic as a threat to the core of the Internet technology itself. Research regarding (non-)effectiveness is important for their lobbying activities. Consequently, the researchers are left asking who should have access to this information and what are the limits to such access? These questions are in line with those asked by security researchers in cases where vulnerabilities are discovered and the responsible party is unresponsive, or unwilling to fix the vulnerability. Corresponding to the initiatives of responsible research and innovation (RRI) in ICT, engaging an ethicist earlier in this research would have been ideal but in practice this ideal is not often met. Accordingly, alongside the ethical analysis described above, this paper aims to show the utility of an ad-hoc ethical appraisal as a means for steering future research of a similar nature along with pointing out areas of concern for improvement.

3.10 Ethical considerations in using information from monitoring file-sharing

Jeroen van der Ham (University of Amsterdam, NL)

Joint work of van Wynsberghe, Aimee; van der Ham, Jeroen
Main reference A. van Wynsberghe, J. van der Ham, "Ethical considerations of using information obtained from online file sharing sites – the case of the PirateBay," in Proc. of ETHICOMP 2014, to appear.
URL http://www.aimeevanwynsberghe.com/uploads/1/4/6/0/14604548/van_wynsberghe_piratebay.pdf

In the Netherlands there have been court-cases which have resulted in Internet Service Providers having to block access to The PirateBay website. It quickly became common knowledge that there were many ways around this blockade. The situation has provided a unique opportunity to measure the effect of block a website.

The measurements have been performed by monitoring the file-sharing process. The participants were identified and categorized per country and ISP. The distribution of peers was measured at different time-points and subsequently analyzed and compared.

The ethical analysis in this case is very complex because of the many different parties involved. In the first place there is the tension between the entertainment industry and consumers who may be obtaining and sharing content illegally. Then, through the court cases and their (in)actions, ThePirateBay and Internet Service Providers became involved in the consideration. Finally the Internet Society Netherlands wanted to protect the general openness and neutrality of the Internet.

Amidst all this the research has been performed while possibly identifying participants in the file-sharing process. I am working with Aimee van Wynsberghe to use this case to improve an ethical analysis framework.

4 Working Groups

The seminar brought together computer scientists, an ethicist and legal scholars to discuss the topic of "ethics in data sharing." After a set of presentations by the participants, some of which are documented in the previous abstracts, there were three main themes requiring ethical attention that were identified by this group of researchers:

- Best Practices and Institutional Review Boards (IRBs) for Ethics in Computer Science,
- Models of Ethics in Producer-Consumer Relations in Data Sharing for Research and Operations, and
- Building Ethical Technology.

The discussions on the first two themes eventually converged. The participants developed a first model for best practice for data sharing.

An online blog or diary was kept by one of the participants (see Section 3.7), and a report describing the model, based on the discussions and case studies, was published in May 2014 [1].

References

1 Sven Dietrich, Jeroen van der Ham, Aiko Pras, Roland van Rijswijk-Deij, Darren Shou, Anna Sperotto, Aimee van Wynsberghe, and Lenore D. Zuck. Ethics in Data Sharing – Developing a Model for Best Practice. In *Proceedings of the 2nd Cyber-security Research Ethics Dialog & Strategy Workshop, IEEE CS Security and Privacy Workshops 2014*, San Jose, CA, May 2014.

Participants

- Jon Callas
Silent Circle – San Jose, CA, US
- Georg Carle
TU München, DE
- Julie E. Cohen
Georgetown University – Washington, DC, US
- Sven Dietrich
Stevens Institute of Technology, NJ, US
- Ronald Leenes
Tilburg University, NL
- Aiko Pras
University of Twente, NL
- Volker Roth
FU Berlin, DE
- Peter Y. A. Ryan
University of Luxembourg, LU
- Jürgen Schönwälder
Jacobs Universität – Bremen, DE
- Darren Shou
Symantec Research Labs – Culver City, CA, US
- Anna Sperotto
University of Twente, NL
- Radu State
University of Luxembourg, LU
- Burkhard Stiller
Universität Zürich, CH
- Jeroen van der Ham
University of Amsterdam, NL
- Roland van Rijswijk-Deij
Radboud Univ. Nijmegen, NL
- Aimee van Wynsberghe
University of Twente, NL
- Da-Wei Wang
Academica Sinica – Taipei, TW
- Sam Weber
Software Engineering Institute – Arlington, VA, US
- Lenore D. Zuck
University of Chicago, IL, US