Introduction: Privacy

Rarely a day goes by in which the term *privacy* fails to make the headlines. Privacy infringements and fundamental discussions of privacy are a part of everyone's agenda. Any inquiry into the future of ubiquitous sensing systems, biosensing included, is challenged to consider privacy from technical, legal, ethical and cultural perspectives.

This overview does not discuss the cadre of internet evangelists who refuse to acknowledge the problem of compromised privacy in the wake of 21st century informatics. Evgeny Morozov's scathing review of the "internet intellectual" Jeff Jarvis in the *Frankfurter Allgemeine Zeitung*[1] is an amusing but mostly sad account of the shoddy scholarship most uncritical internet advocates represent – and propagate.

The collection of papers described here falls into two main categories: those that represent privacy as fundamentally a technically solvable problem, and those that define privacy as a legal/cultural issue. The first category aptly proposes technical solutions, varying in complexity, to both small and large privacy problems. The second group shifts the discussion out of the technical arena and into the legal and policy arena, where institutional regulation and consensus-based control are proposed as more viable and socially robust solutions.

Of the papers that propose technical solutions to privacy matters, some deal with hardware, some with software and others with protocol issues. One often proposed approach in network trace analysis, for example, is to obfuscate sensitive data by selectively adding noise[2] while maintaining the computability of statistically significant aspects of the data streams. The implementation of this approach varies widely. One research group describes a system that obfuscates the location of sensor nodes in a sensor network, making eavesdropping impossible[3]. The authors describe in detail a system that hides the destination node by adding dummy nodes through a series of fictitious nodes and obfuscating the data path from source to destination while maintaining energy efficient operation. Here the term privacy is similar in meaning to the term secrecy, to be understood in a military-control setting where the goal is to prevent the unauthorized collection of data. Encryption keys and the culture of encryption share a similar interpretation of privacy.

Within the privacy-equals-secrecy paradigm, some researchers have focused on adding context and location awareness to privacy enhancement strategies. One experiment describes an indoor location aware system with high density wireless monitoring. The privacy enabling algorithm calculates a person's position on a continuous coordinate grid (assuming signal strength maps linearly to distance). Then the resulting coordinates are mapped onto real space coordinates using

[1] http://www.faz.net/aktuell/feuilleton/netzdiskurs-das-elend-der-internetintellektuellen-11504372.html

[2] McSherry, F., Mahajan, R., "Differentially-Private Network Trace Analysis," Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM, 2010, p. 123-134

[3] Qijun Gu, Xiao Chen , "Privacy Preserving Mobility Control Protocols in Wireless Sensor Networks," I-SPAN 2008, 7-9 May 2008, p.159-164

a set of trained values. Because users can decide if their location is transmitted, the system, according to the authors, respects privacy[4].

More recently, researchers have attempted to create an adaptive privacy system based on a *territorial privacy* model. The approach is similar to that used in *geo-fencing*[5], where one controls the extent of (virtual) territory by limiting Wi-Fi coverage of the network to specific physical boundaries. Here, however, territorial privacy specifically includes a person's right to be left alone; allowing for a state in which a person is able to perceive his/her extended territory, and is able enforce it by allowing only desired participants access, excluding disturbers (whether human or machine). This is clearly a more nuanced privacy concept that goes beyond the secrecy concept. It includes a quality of being, and attaches this to locations – and hence situations – in which privacy is to be established and enforced. The authors describe the various environment types in which this model could be effective, and they range from highly private spaces, to shared private spaces, shared environments and public environments[6]. Despite this differentiated privacy concept, the decision process by which private spaces are to be distinguished from public ones, for example, remains vague.

Yet another technology-based privacy design suggests an *ontology-centric approach* to managing privacy. This paper is interesting as it proposes a technical framework with a mixed human-computer model for privacy transgression oversight while leaving the final decision on how to respond in individual cases in the hands of a person. Here, the researchers point out that 'hardcoded' solutions make it difficult to trace whether a system is considering a given privacy regulation, and this makes it challenging to modify privacy policies. In response to this dilemma they propose a privacy design framework with two additional modules, one computational and one human: a privacy manager module, and a human supervisor. Importantly, the privacy manager model includes an ontology that represents the German Federal Data Protection Act (*Bundesdatenschutzgesetz*), and is augmented by a human in the loop, a data protection officer[7] who is in charge of oversight and assistance in difficult cases. The authors justify this approach with the observation that a human being can add real-world knowledge and address special individual rights in ways synthetic systems cannot.

On the opposite end of the privacy design spectrum one finds the approaches that deemphasize technology and focus on long-established ideas of personhood, the private and public realms and human rights. In Europe, sociologists and political scientists have been concerned with the impact of ambient intelligence (the continental version of the US ubiquitous computing) technologies on privacy for several years. Consequently, attempts at addressing privacy and data protection challenges have generated sophisticated responses from a growing collection of disciplines. The text by Antoinette Rouvroy published in "Studies in Ethics, Law and

[4] Smailagic, A., Kogan, D. "Location Sensing and Privacy in a Context-Aware Computing Environment," Wireless Communications, IEEE, Vol. 9, Iss. 5, Oct. 2002, p. 10-17

[5] Eyal, D., LaMarca, A., Satyanarayanan, M., Location Systems: An Introduction to the Technology Behind Location Awareness. Morgan & Claypool Publishers, 2008.

[6] Konings, B., Schaub, F. "Territorial Privacy in Ubiquitous Computing," Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on, 2011, p. 104-108

[7] Abou-Tair, D., Berlik, S., An ontology-based approach for managing and maintaining privacy in information systems, PROCEEDINGS, Lecture Notes in Computer Science, Vol. 4275, pp. 983-994, Springer, 2006

Technology"[8] defines privacy in the context of data collection of all kinds: Privacy and data protection are complementary legal instruments aimed at protecting an individual's possibility to construct his/her own identity and personality without unreasonable constraints. The concept includes an individual's ability to control some aspects of his/her identity that he/she projects on the world. The distribution of agency that characterizes ambient intelligence systems is seen by the author as a threat to the fundamental value grounding both privacy and data protection laws: Respect for individual autonomy. The author argues that the relevance, applicability and adequacy of the European privacy and data protection legal frameworks to deal with those unprecedented challenges requires, a re-thinking of the normative grounds of what is meant by the 'right to privacy'. Privacy, it is argued, is an instrument for fostering the specific yet changing autonomic capabilities of individuals that are, in a given society at a given time, necessary for sustaining a healthy democracy. The author challenges the reader to consider, for example, how laws should preserve the conditions for individual reflexive autonomy and self-determination against incentives for anticipative conformity ensuing from monitoring and profiling through surveillance systems. The author points out that most of these problems stem from ambient systems' need for information about 'users' and the framing of personal information as a commodity. This is inscribed into the procedures used by ambient systems. The author lists the example of classifying people into groups (as advanced surveillance might) and normalizing the population in groups with 'technical paternism'. The author points out that the right to privacy is more than just the right to be left alone; it includes the right to self-determination, disallowing paternalism from the state. Thus the author interprets the right to privacy as autonomy in the construction of one's identity (explicit in the European human rights framework, but not in the United States). Additionally, the text discusses deep ethical and legal issues. The author asks, for example: How can one assign responsibilities in computer-controlled environments with potential damages resulting from combined agencies? The author suggests that the technical class of ambient system designers accept the inherently political nature of their work. Unfortunately, there is no attempt to reach out across the disciplinary divide and propose practical, realizable solutions to specific problems.

Clearly, the discussion around Big Data is one that cannot be held seriously without considering privacy issues. To this topic danah boyd has cogently written and spoken. In a recent presentation,[9] Boyd laid out the connection between the big data and privacy in five succinct points. 1) Sampling approaches are important and problematic. Large data samples do not guarantee representative data samples, and big data seduces data collectors into believing that what can be collected represents the general population; 2) Not all data are created equal. Big data introduces two new networks derived from data traces: Articulated social networks and behavioral social networks (which are different from the data sociologists collect); 3) Every act of data analysis (whether quantitative or qualitative) involves interpretation; there is no fully objective way of analyzing data collected on people; 3) Privacy is about context, and methodology is about working out context in which data is collected and analyzed, considering how this will affect people. The author makes the point that just because data is accessible does not guarantee that it will generate any good for the public; 4) Privacy is premised on a collective

[8] Rouvroy, A., "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence," Studies in Ethics, Law and Technology: Vol. 2: Iss. 1, Article 3, 2008

[9] Boyd, D., "Privacy and Publicity in the Context of Big Data." WWW. Raleigh, North Carolina, April 29 2010.

understanding of a (social) institution's boundaries. Where such a collective understanding is ill-formed or one-sided, privacy will not be maintained or engrained in to the social fabric and probably not be enforced by institutions. In sum, the author makes a strong argument for the claim that privacy will never be encoded in ones and zeros alone.

Further Reading:

- Abou-Tair, D., Berlik, S., An ontology-based approach for managing and maintaining privacy in information systems, PROCEEDINGS, Lecture Notes in Computer Science, Vol. 4275, pp. 983-994, Springer, 2006
- Donath, J., and Boyd, D., "Public displays of connection." BT Technology Journal 4 (Oct. 2004): 71-82. Web. 23 Nov. 2004.
- Konings, B., Schaub, F. “Territorial Privacy in Ubiquitous Computing,” Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on, 2011, p. 104-108
- Qijun, G., Xiao, C, , "Privacy Preserving Mobility Control Protocols in Wireless Sensor Networks," I-SPAN 2008, 7-9 May 2008, p.159-164
- *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, Eds. Christian Fuchs, Kees Boersma, Anders Albrechtslund, Marisol Sandoval, New York: Routledge Press, 2011.
- Namatame, N., Nakazawa, J., Takashio, K., Tokuda, H. “Life2Guard: A Physical Disorder Detection in Private Rooms,” Applications and the Internet, 2008. SAINT 2008. International Symposium on, 2008, p. 177-180
- Rouvroy, A., “Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence,” Studies in Ethics, Law and Technology: Vol. 2: Iss. 1, Article 3, 2008
- Staff, FTC, “Protecting Consumer Privacy in an Era of Rapid Change–A Proposed Framework for Businesses and Policymakers,” Journal of Privacy and Confidentiality, Vol. 3,Iss. 1, Article 5, 2010.
- Smailagic, A. and Kogan, D. “Location Sensing and Privacy in a Context-Aware Computing Environment,” Wireless Communications, IEEE, Vol. 9, Iss. 5, Oct. 2002, p. 10-17