

PROP-ID

Appendix A Literature Review

II. ANNOTATED BIBLIOGRAPHY

Introduction

An Overview of this Annotated Bibliography

To supplement the research that we conducted into global digital wallet developments, we read many web articles and peer-reviewed academic papers. These sources allowed us to gain a deeper understanding of the issues relating to digital wallet deployment. For example, two papers by Mallat & Tuunainen (2008) and Morawczynski & Miscione (2008) were particularly helpful in emphasizing the importance of establishing trust in the effective deployment of a mobile payment system. Morawczynski & Miscione analyzed a case study – the M-PESA mobile payment system in Kenya – and found that interpersonal trust between customers and merchants was a major reason for its success. By foregrounding the importance of preventing the unnecessary disclosure of personal information, we believe that the Prop-ID app would enable merchants in other countries to establish this all-important trust link with customers.

A major objective of the Prop-ID project has been to be critical about certain merchant ID practices, such as card swiping and barcode scanning. The OPC case studies that we identified were helpful in providing empirical evidence of these practices happening in Canada. We were able to locate two helpful academic papers by Cross (2005) and Palmer et al. (2010) that take a critical look at the ongoing practice of ID card swiping. Another detrimental result of rampant data collection that our Prop-ID initiatives react against is identity theft. The paper by Copes & Vieraitis (2009) provides insight into some of the most common ways in which this crime is committed.

We have also tried to be very critical about the thriving but poorly understood data brokerage industry and the data profiling practices that it employs. Some of the most helpful sources that we have identified in this area include a CIPPIC report from 2006 that thoroughly explains the data brokerage industry and a paper by Manzerolle & Smeltzer (2011) that concentrates on the negative economic and societal effects created by the commercial exploitation of databases. The two papers by King & Jessen (2010) are about consumer profiling and behavioural advertising specifically in the mobile phone

industry. Rather than simplistically declaring that consumer profiling should be done away with, the Prop-ID project has been interested in helping to make such practices more citizen-centric as digital wallet technology becomes more widespread.

As the technology is still very nascent, identifying high quality academic papers about digital wallet development has been challenging. A paper out of Singapore by Balan et al. (2009) perhaps represents the best academic analysis of a digital wallet project that we have been able to find. This paper documents the evolution of a digital wallet application called mFerio. A magazine article by Martin (2011) also offers a helpful, in-depth analysis of the technical considerations relating to digital wallet deployment.

As privacy is a very ambiguous word with multiple possible definitions, we also carefully read a number of papers dealing specifically with notions of privacy. We felt it important to determine for ourselves exactly how we use that word on the Prop-ID project. Out of the papers we read, we have found that we identify closely with the notions of privacy outlined in the Nissenbaum (2004) and Solove (2007) papers. That is, the Prop-ID project does not subscribe to the Brandeis notion that privacy is merely about “the right to be let alone.” Rather, privacy is about respecting contextual integrity and clearly defining norms of appropriateness in various settings so that we may interact more fully and democratically with society.

Finally, the core element behind the design of our Prop-ID digital wallet application is selective disclosure. We have been able to identify a number of other projects that also incorporate this approach of allowing citizens to disclose only the personal information that is absolutely essential for a particular transaction or verification. Some of these projects use different terminology, but the concept is essentially the same. For example, the Le Metayer & Monteleone (2009) paper makes reference to a software architecture called Privacy Agents, which embodies the same principles as selective disclosure.

Table of Contents

Author and Title by order of appearance (page numbers in gutter)

- 5 **Anderson, R.** (2011). Can We Fix the Security Economics of Federated Authentication?
- Andrejevic, M.** (2009). Control over personal information in the database era.
- Balan, R.K., Ramasubbu, N., Prakobphol, K., Christin, N. & Hong, J.** (2009). mFerio: the design and evaluation of a peer-to-peer mobile payment system.
- Bernard, T.S. and Miller, C.C.** (2011). Swiping is the easy part.
- 6 **Bolton, M.** (2011). NFC in phones: what you need to know.
- Bosker, B.** (2011). Google's Digital Wallet: Why Google Wants To Reinvent How You Pay.
- Brands, S.** (2010). U-Prove Technology Overview.
- Canadian Internet Policy and Public Interest Clinic.** (2006). On the Data Trail: how detailed information about you gets into the hands of organizations with whom you have no relationship, A Report on the Canadian Data Brokerage Industry.
- 7 **Cavoukian, A. and Prosch, M.** (2010). The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users.
- CBC News.** (2011). Visa pitches 'digital wallet'.
- Choi, D., Roh, J., Kim, S. & Jin, S.** (2009). Identity Data Security System for the Digital Identity Wallet.
- Cleff, E.B.** (2010). Effective approaches to regulate mobile advertising: Moving towards a coordinated legal, self-regulatory and technical response.
- 8 **Copes, H. and Vieraitis, L.M.** (2009). Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes.
- Cross, J.T.** (2005). Age Verification in the 21st Century: Swiping Away Your Privacy.
- da Costa, B., Schulte, J., & Singer, B.** (2006). Surveillance Creep! New Manifestations of Data Surveillance at the Beginning of the Twenty-First Century.
- 9 **Fujitsu.** (n.d.). Technology Perspectives – A thought-provoking look at key forces of change (excerpt).
- Future of IDENTITY in the Information Society.** (n.d.). Study on Mobile Identity Management.
- Gadzheva, M.** (2008). Privacy in the Age of Transparency: The New Vulnerability of the Individual.
- Genosko, G. and Thompson, S.** (2006). Administrative surveillance of alcohol consumption in Ontario, Canada: pre-electronic technologies of control.
- 10 **Gerdes Jr., J.H., Kalvenes, J., & Huang, C.** (2009). Multi-dimensional credentialing using veiled certificates: Protecting privacy in the face of regulatory reporting requirements.
- Godoe, H. and Hansen T.B.** (2009). Technological regimes in m-commerce: Convergence as a barrier to diffusion and entrepreneurship?
- Gosselin, S.** (2011). QR Codes vs. Near Field Communications: Do you need to choose?
- 11 **Gurses, S.** (2010). PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm.
- Halperin, R. & Backhouse, J.** (2008). A roadmap for research on identity in the information society.
- Hodel-Widmer, T.B.** (2006). Designing databases that enhance people's privacy without hindering organizations.
- Hornung, G. and Schnabel, C.** (2009). Data protection in Germany I: The population census decision and the right to informational self determination.
- 12 **Karyda, M., Gritzalis, S., Park, J.H. & Kokolakis, S.** (2009). Privacy and fair information practices in ubiquitous environments: Research challenges and future directions.

Table of Contents

Author and Title by order of appearance (page numbers in gutter)

King, N.J. and Jessen, P.W. (2010a).

Profiling the mobile customer - Privacy concerns when behavioural advertisers target mobile phones - Part I.

King, N.J. and Jessen, P.W. (2010b).

Profiling the mobile customer - Is industry self-regulation adequate to protect consumer privacy when behavioural advertisers target mobile phones? - Part II.

13

Krumm, J. (2011). Ubiquitous

Advertising: The Killer Application for the 21st Century.

Kwang, K. (2011). Swift mobile wallet

adoption hinges on apps.

Le Metayer, D. & Monteleone, S.

(2009). Automated consent through privacy agents: Legal requirements and technical architecture.

Mallat, N. & Tuunainen, V.K. (2008).

Exploring Merchant Adoption of Mobile Payment Systems: An Empirical Study.

14

Martin, Z. (2011). The mobile as a credential.

Manzerolle, V. & Smeltzer, S. (2011).

Consumer Databases and the Commercial Mediation of Identity.

Michelfelder, D.P. (2010). Philosophy,

Privacy, and Pervasive Computing.

15

Mobio. (n.d.). Mobio — Empowering Identity.

Morawczynski, O. & Miscione, G.

(2008). Examining trust in mobile banking transactions: the case of M-PESA.

Mydex. (n.d.). Mydex.

Nissenbaum, H. (2004). Technology, Values, and the Justice System: Privacy and Contextual Integrity.

16

OECD Directorate for Science,

Technology and Industry. (2007). At a Crossroads: Personhood and Digital Identity in the Information Society.

Office of the Privacy Commissioner of Canada. (2008). Background – Ticketmaster Investigation.

Office of the Privacy Commissioner of Canada. (2008). Identification machines and video cameras in bars examined.

17

Office of the Privacy Commissioner of Canada. (2009). Fraud detection not an acceptable reason to collect driver's licence numbers for store memberships.

Palmer, D., Warren, I. and Miller, P.

(2010). ID scanners in the night time economy.

Patten, G. (2010). Guilt by Association: Canada, Identity Cards and the Myth of Privacy.

Perez, S. (2011). NFC in 2011: Who's building your mobile wallet?

18

Rauhofer, J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society.

Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining.

Shilton, K. (2010). Participatory Sensing: Building Empowering Surveillance.

Solove, D.J. (2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy.

19

Stalder, F. (2002). Privacy is not the antidote to surveillance.

Stoddart, E. (2008). Who watches the watchers? Towards an ethic of surveillance in a digital age.

Swilley, E. (2010). Technology rejection: the case of the wallet phone.

20

Taylor, J.A., Lips, M. & Organ, J. (2008). Identification practices in government: citizen surveillance and the quest for public service improvement.

University of Freiburg. (n.d.). Online-Demonstration des ID-Managers.

Wladawsky-Berger, I. (2011). The evolution of money.

Topic Index

Page Number and Author

Ambient Intelligence

- 9 Gadzheva
- 12 Karyda et al

Card Swiping

- 5 Bernard & Miller
- 8 Cross
- 8 da Costa et al
- 16 OPC Canad Inns
- 17 OPC Fraud
- 17 Palmer et al

Database

- 5 Andrejevic
- 11 Hodel-Widmer
- 14 Manzerolle & Smeltzer
- 16 OPC Canad Inns
- 17 OPC Fraud
- 18 Shilton
- 19 Stoddart

Data Brokerage

- 6 CIPPIC
- 8 da Costa et al
- 14 Manzerolle & Smeltzer

Data Profiling

- 6 CIPPIC
- 9 Gadzheva
- 9 Genosko & Thompson
- 12 King & Jessen
- 13 Krumm
- 14 Manzerolle & Smeltzer
- 16 OPC Ticketmaster
- 17 Palmer et al
- 17 Patten
- 18 Rauhofer
- 18 Schermer
- 18 Solove
- 20 Taylor et al

Data Protection

- 11 Hornung & Schnabel
- 16 OECD
- 18 Rauhofer
- 18 Schermer
- 18 Solove

Digital/Mobile Wallet

- 5 Anderson
- 5 Balan et al
- 5 Bernard & Miller
- 6 Bolton
- 6 Bosker
- 7 CBC
- 7 Choi et al
- 9 Fujitsu

- 9 FIDIS
- 10 Godoe & Hansen
- 10 Gosselin
- 13 Kwang
- 13 Mallat & Tuunainen
- 14 Martin
- 15 Mobio
- 15 Morawczynski & Miscione
- 17 Perez
- 19 Swilley
- 20 Wladawsky-Berger

Federated Authentication

- 5 Anderson
- 5 Balan et al
- 6 Brands
- 7 Choi et al
- 14 Martin
- 16 OECD

Identity Management

- 5 Balan et al
- 6 Brands
- 7 Choi et al
- 11 Halperin & Backhouse
- 15 Mobio
- 15 Mydex
- 16 OECD

Identity Theft

- 6 CIPPIC
- 8 Copes & Vieraitis
- 8 Cross

Liquor Control Board of Ontario (LCBO)

- 9 Genosko & Thompson

Mobile Advertising

- 6 Bosker
- 7 Cleff
- 13 Krumm

Near-Field Communication (NFC)

- 5 Balan et al
- 6 Bolton
- 10 Gosselin
- 13 Kwang
- 14 Martin
- 17 Perez

Participatory Sensing

- 18 Shilton

Privacy

- 7 Cavoukian & Prosch
- 7 Cleff

- 9 FIDIS
- 9 Gadzheva
- 10 Gerdes et al
- 11 Gurses
- 11 Hodel-Widmer
- 11 Hornung & Schnabel
- 12 Karyda et al
- 12 King & Jessen
- 13 Krumm
- 13 Le Metayer & Monteleone
- 14 Manzerolle & Smeltzer
- 14 Michelfelder
- 15 Nissenbaum
- 16 OECD
- 16 OPC Ticketmaster
- 16 OPC Canad Inns
- 17 OPC Fraud
- 17 Patten
- 18 Rauhofer
- 18 Schermer
- 18 Shilton
- 18 Solove
- 19 Stalder
- 20 Taylor et al

Quick Response (QR) Code

- 10 Gosselin
- 15 Mobio

Selective Disclosure

- 6 Brands
- 9 FIDIS
- 10 Gerdes et al
- 13 Le Metayer & Monteleone
- 14 Michelfelder
- 15 Mobio
- 15 Mydex
- 16 OECD
- 18 Shilton

Solidarity

- 19 Stoddart

Subsidiarity

- 19 Stoddart

Trust

- 13 Mallat & Tuunainen
- 14 Martin
- 15 Morawczynski & Miscione
- 19 Swilley

Ubiquitous Computing

- 12 Karyda et al
- 13 Krumm
- 14 Michelfelder

Anderson, R. (2011). Can We Fix the Security Economics of Federated Authentication? University of Cambridge, 1–8.

Anderson analyzes the potential shortcomings of federated authentication in the mobile wallet space and proposes a number of regulatory solutions. First, Anderson briefly discusses the four main types of federated authentication technology deployed thus far – SSO, SSL, 3DS and OpenID. He points out reasons why these technologies have all failed to truly catch on. Mobile wallets will be based on an architecture with four layers – the secure element (SE), the phone itself, an online service for backup and a trust services manager for key verification. Anderson suggests that in order to make a mobile wallet system work efficiently, the incentives of the various firms involved (e.g. banks, phone companies, card providers) need to be aligned. He provides some suggestions on how governments can do this. (p. 5) Federated authentication has failed, he suggests, because these incentives were misaligned.

Andrejevic, M. (2009). Control over personal information in the database era. *Surveillance & Society*, 6(3), 322–26.

This is a short commentary on the UK government report *Surveillance: Citizens and the State* from 2009. It credits the report for calling attention to the need for increased citizens awareness of these issues but also criticizes it for posing a simple dichotomy between liberty and surveillance. Citing Lyon, among others, Andrejevic makes the point that we cannot antagonize surveillance in order to develop appropriate solutions. He points out the numerous beneficial uses of surveillance, such as its role in “allocating resources, protecting citizens, and the process of collective self-governance.” The consequences of the privatization of information collection, e.g. reduced accountability, are discussed. Andrejevic calls for a shift from personal autonomy to collective autonomy. (p. 323) These ideas are all in line with the Prop-ID project. Great line: “Control over personal information is the database era analogue of control over labour power in the industrial revolution.”

Balan, R.K., Ramasubbu, N., Prakobphol, K., Christin, N. & Hong, J. (2009). mFerio: the design and evaluation of a peer-to-peer mobile payment system. *Proceedings of the The 7th Annual International Conference on Mobile Systems, Applications and Services (MobiSys)*, 1–14.

This technical paper produced by engineering research teams from Singapore Management University and Carnegie Mellon documents the development of an NFC-based digital wallet application called mFerio. A step-by-step breakdown of how the app would work is provided in section 3.4 of the paper. The authors are critical about public key cryptography and ultimately decide that it isn't suitable for certain phones. The authors conducted an empirical study by documenting the responses of 104 users to the digital wallet app. The feedback was mostly optimistic - users found that the app lowered cognitive load in certain situations, compared to cash.

Bernard, T.S. and Miller, C.C. (2011). *Swiping is the easy part*. Retrieved on April 25, 2011.

[HTTP://WWW.NYTIMES.COM/2011/03/24/TECHNOLOGY/24WALLET.HTML](http://www.nytimes.com/2011/03/24/technology/24wallet.html)

This article describes the ongoing battle between various stakeholders in the mobile wallet domain, primarily in the United States. The authors suggest that the success of mobile wallets in Japan might be because it has a single dominant mobile carrier and small number of banks. In the US, however, the field is more fragmented: telcos, banks, card issuers and platform providers are all vying for control over a mobile payment system and seem reluctant to agree on anything. It is suggested that Verizon, AT&T and T-Mobile all agreed to form ISIS out of frustration at negotiating with the banks. The banks and card issuers have thus far been able to avoid working with the telcos by using stickers and microSD cards to make phones NFC-capable. But as more phones become embedded with NFC capability, the banks will perhaps feel more compelled to cooperate with the telcos.

Bolton, M. (2011). NFC in phones: what you need to know. Retrieved on April 27, 2011.

[HTTP://WWW.TECHRADAR.COM/NEWS/PHONE-AND-COMMUNICATIONS/NFC-IN-PHONES-WHAT-YOU-NEED-TO-KNOW-948410](http://www.techradar.com/news/phone-and-communications/nfc-in-phones-what-you-need-to-know-948410)

This article provides a thorough explanation of near field communication (NFC) technology with specific reference to mobile phones. NFC is not new technology and is actually based on RFID. Bolton describes three different uses for NFC: sharing, pairing and transactions. The contactless payment capability has been garnering the most attention. When paying via NFC chip with a phone, the customer can receive back digital information in the form of coupons, loyalty cards, receipts, etc. These ads would be very targeted because the store(s) will know the customer's transaction history through NFC. This is mentioned uncritically and is a practice that the Prop-ID project wants to question. This data aggregation opportunity is likely why Google decided to support NFC. Bolton suggests that Google didn't have a concrete business plan for NFC in the Nexus S but included it more as a 'future-proofing' move for the device. Bolton also provides arguments countering the widespread conception that NFC poses major security concerns.

Bosker, B. (2011). Google's Digital Wallet: Why Google Wants To Reinvent How You Pay. Retrieved on May 26,

2011. [HTTP://WWW.HUFFINGTONPOST.COM/2011/05/25/GOOGLES-NFC-DIGITAL-WALLET_N_867051.HTML](http://www.huffingtonpost.com/2011/05/25/googles-nfc-digital-wallet_n_867051.html)

This article clearly, although uncritically, outlines many of the privacy concerns relating to the deployment of digital wallet technology. It specifically focuses on Google's upcoming digital wallet, which will allow Google to tap into an even broader range of personal information about its users than it already has access to via online services. Now, Google will collect information about one's point-of-sale purchasing decisions and use that to strengthen its advertising initiatives. For example, the Google digital wallet will collect a user's shopping history and advertise products to that user based on the history. Merchants will also potentially have access to this data. The Prop-ID project is interested in being critical about these targeted advertising practices and introducing into this market an element of privacy discourse that seems to be missing.

Brands, S. (2010). U-Prove Technology Overview. Microsoft Corporation, 1–19. PDF file.

This overview provides a thorough explanation of the U-Prove cryptographic identity management technology. It provides a summary of the basic features of the protocol, along with illustrative graphics. The U-Prove technology has been helpful as a reference point for us in designing the various prototypes of our Prop-ID smartphone app. The cryptography captures the same general principles that the Prop-ID project promotes, particularly selective disclosure. Section 4.3 of the paper specifically discusses selective disclosure.

Canadian Internet Policy and Public Interest Clinic. (2006). On the Data Trail: how detailed information about you gets into the hands of organizations with whom you have no relationship, A Report on the Canadian Data Brokerage Industry. PDF file.

This is the most comprehensive and specific analysis of data collecting practices that I have been able to find. The report explains how data are commonly collected and disseminated across companies. It provides a "data supply chain" diagram on page 7 to illustrate the data flow from individual to data owner to data agent to data user. These definitions could be used by Prop-ID to reveal to the public exactly what happens in data collection. ChoicePoint, an American data brokerage, is mentioned as an example of poor data handling by a corporate entity. (p. 4) The company has been associated with hundreds of identity theft cases. Important questions for future research are offered at the end of the report. (p. 47)

Cavoukian, A. and Prosch, M. (2010). The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users. PDF file.

This document does a good job explaining the importance of developing privacy-enhancing technologies (PETs) for mobile phones. Some striking statistics are provided, e.g. “in North America, it is estimated that there are 94 cell phone subscriptions for every 100 individuals, while in Europe, there are 120 subscriptions per 100 people.” Cavoukian’s 7 principles of PbD are applied to mobile phone technology. (p. 5) Advice on building privacy into mobile phones is provided to specific stakeholders: manufacturers, OS developers, network providers, app developers and users. The Prop-ID project fits a number of the goals that this document sets forth, e.g. “design applications with privacy in mind.” Concepts in the document to be explored further: transformative technologies, privacy wizard, informed consent, standards for security. Cavoukian and Prosch recommend that app developers “employ notice and informed consent” to make users aware of how personal information will be used and stored. Prop-ID should consider this notion – how long will the data profiles be held and how will this information be protected?

CBC News. (2011). Visa pitches ‘digital wallet’. Retrieved on May 13, 2011.

[HTTP://WWW.CBC.CA/NEWS/TECHNOLOGY/STORY/2011/05/11/TECHNOLOGY-VISA-DIGITAL-WALLET.HTML](http://www.cbc.ca/news/technology/story/2011/05/11/technology-visa-digital-wallet.html)

Visa is working on deploying a PayPal-like online digital wallet in which customers can centralize their financial data to make online shopping transactions. The company eventually wants to expand into smartphone digital wallets in which customers can make in-person transactions at stores using contactless technology such as NFC. The centralization of personal information that Visa proposes should perhaps be concerning. Visa claims its digital wallet will not hold ID, e.g. driver’s license, health card. This, however, might be more of a missed opportunity than a positive trait. The Prop-ID project encourages the incorporation of ID data into digital wallets, with the appropriate privacy-enhancing mechanisms in place.

Choi, D., Roh, J., Kim, S. & Jin, S. (2009). Identity Data Security System for the Digital Identity Wallet. International Conference on Advanced Communication Technology, 3, 1678–1681.

This technical paper provides a look at the digital wallet work being done by researchers in South Korea. The authors provide technical explanations for how their system would work. The paper is useful in providing an explanation on how to counteract a potential vulnerability in a digital wallet system. When a wallet is stolen or acquired by a malicious third party, what happens? The authors propose a system that allows for suspension of accounts and/or backup and recovery of identity data.

Cleff, E.B. (2010). Effective approaches to regulate mobile advertising: Moving towards a coordinated legal, self-regulatory and technical response. Computer Law & Security Review, 26, 158–169.

Cleff points out the limitations of relying on either a legal, self-regulatory or technical response to abuses of personal information by the mobile advertising industry. She suggests that a combination of these practices might be the best approach. Most privacy laws, such as EU’s Data Protection Directive, are based on four principles: necessity, finality, transparency and proportionality. Cleff suggests that the main problem with privacy-enhancing technologies (PETs) is that few people use them. Seemingly simple PETs might still be too complex for many users and they might slow down the mobile device. But Cleff, quoting Solove, points out the need for PETs that allow users to stipulate the use of only parts of their personal information for certain reasons. The Prop-ID app would address this need.

Copes, H. and Vieraitis, L.M. (2009). Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes. *Criminal Justice Review*, 34(3), 329–349.

This revealing paper problematizes a number of popular assumptions regarding identity theft. Mainly, it is commonly assumed that identity theft is a white collar crime perpetrated by business professionals. But empirical evidence reveals that this simply isn't the case - identity theft perpetrators come from all walks of life. Particularly relevant to Prop-ID is that the article describes common ways in which identity theft is committed. The crime was often facilitated by corrupt employees who used internal company records to collect personal information with the intention to either commit identity theft themselves or sell the information to the perpetrator. These corrupt employees often came from powerful institutions like banks and government agencies. One popular form of identity theft is to collect personal information from a person's driver's licence and other ID cards in order to setup a credit card account in their name. This paper convincingly establishes the Prop-ID notion that only information essential to a transaction should be provided and that no institution, even the most official, should be trusted blindly with one's personal information.

Cross, J.T. (2005). Age Verification in the 21st Century: Swiping Away Your Privacy. *The John Marshall Journal of Computer & Information Law*, 363, 1–59.

This paper provides a balanced look at the practice of ID card swiping, particularly within the United States. Various states have created legislation to regulate ID swiping, e.g. Ohio, New Hampshire, New York. Cross argues that state legislation has proved to be too inconsistent and federal measures are required. Federal laws, such as the Driver's Privacy Protection Act of 1994, have been useful but are too limited in scope. Cross provides useful technical explanations of the differences between magnetic strips and two-dimensional barcodes. Cross shows that card swiping in the US has largely not been conforming to the FTC's fair information practice principles. But he also acknowledges the potential benefits of card swiping, e.g. reduced selling to minors. Cross discusses how identity theft is often committed with the information gathered from card swiping. Cross recommends that we also look at the manufacturers of the card swiping equipment and think about possible industry standards to put in place. Cross acknowledges that the information gathered from card swiping is often used for marketing purposes, but somewhat trivializes this practice by calling it a lesser problem. But the Prop-ID project recognizes that such marketing practices can actually detrimentally affect one's life chances.

da Costa, B., Schulte, J., & Singer, B. (2006). Surveillance Creep! New Manifestations of Data Surveillance at the Beginning of the Twenty-First Century. *Radical History Review*. 95: 70–88.

This paper provides a critique of Automatic Identification and Data Capture (AIDC) practices. It is primarily American in focus, but many of the concepts and principles relate to Prop-ID. The problematic consequences of using driver's licenses with card readers are discussed. Some interesting data dissemination horror stories are also provided, (p. 80) such as when many blacks in Florida were denied their voting rights because of work conducted by data broker ChoicePoint that propagated faulty, unverified data. Loyalty cards are also discussed. In addition to this paper, the authors created the Swipe project, which demystifies the data collection business by providing tools such as "Decode Your Barcode" that enable people to understand the value of their information. Similar to our overlays, they have also created "stickers for people to place over their magnetic stripe or bar code on drivers' licenses that have slogans such as 'Keep your paws off my databody' or 'I stop shopping when you start swiping.'"

Fujitsu. (n.d.). Technology Perspectives – A thought-provoking look at key forces of change (excerpt). PDF file.

This corporate document is useful to Prop-ID in emphasizing the importance of mobile-focused research. Fujitsu predicts that smartphone use will reach global ubiquity within a few years and people will become more and more interested in mobile transactions. It reads, “the smartphone will become the global ‘common denominator’ for consumer transactions.”

Future of IDentity in the Information Society. (n.d.). Study on Mobile Identity Management. Retrieved February 22, 2011.

[HTTP://WWW.FIDIS.NET/RESOURCES/DELIVERABLES/HIGHTECHID](http://www.fidis.net/resources/deliverables/hightechid)

The iManager project from University of Freiburg is very similar to the Prop-ID project. It is also a privacy-enhancing technology for mobile users. This is not a recent project – it was presented at the European IT show CeBIT in 2003. The idea behind iManager is to allow mobile users to be more selective about the information that they release. This is accomplished by creating multiple profiles for different ID scenarios. The technical architecture is based on the P3P and JAP privacy protocols. The webpage also addresses what happens when there is a conflict between what the user specifies and what the service requests. This is referred to as identity negotiation. “iManager informs the user of this conflict and proposes solutions like a suitable partial identity for solving it.”

Gadzheva, M. (2008). Privacy in the Age of Transparency: The New Vulnerability of the Individual. Social Science Computer Review, 26(1), 60–74.

Gadzheva suggests that the ongoing development of ambient intelligence (Aml) technologies threatens to leave people without any control over their personal information. With Aml, the information processing power of technology becomes truly invisible. People do not realize what exactly is happening behind the scenes whenever they use a function on their mobile phone, for instance. They do not understand the consequences of the data profiling facilitated by Aml technologies. But this profiling often affects one’s life chances. There is controversy as to whether or not the information collected by Aml should be considered “personal data” because it can’t always identify a person. But Gadzheva stresses that data brokers are not usually interested in individuals, anyway – they are interested in classifying individuals into particular groups. This type of surreptitious classification can lead to a loss of control on part of the citizen. Gadzheva suggests that rather than reducing the amount of data collected, we should instead focus on empowering people with more control over how their data are processed. The Prop-ID project slightly disagrees in that we think there is value in reducing the collection of unnecessary data. Finally, Gadzheva recommends that new technologies be developed for protecting privacy, especially in the mobile space where lengthy, traditional privacy policies are not feasible. But, Gadzheva says, technical developments are not sufficient. We must also build legal, regulatory and self-regulatory mechanisms to complement the technologies.

Genosko, G. and Thompson, S. (2006). Administrative surveillance of alcohol consumption in Ontario, Canada: pre-electronic technologies of control. Surveillance & Society, 4(1/2), 1–28.

This paper uses the Liquor Control Board of Ontario (LCBO) as a case study to explore how public sector organizations administer their social control mandate. The LCBO, in particular, has long employed well-disguised technologies to aid in carrying out its social control mandate. The technologies documented in this paper include permit books, punch cards and comprehensive lists. The LCBO used various techniques to carry out social sorting from about 1927 into the late 60s. First Nations and Inuit peoples were particularly ostracized through these practices; a “drunk list” was established that barred many from purchasing alcohol. This drunk list was determined by sometimes very questionable statistical analysis. Often, people –

particularly minorities – were placed on this list without having done anything wrong. But statistical analysis had determined that “their intemperance had become a predictable part of a future already over,” evoking thoughts of Philip K. Dick’s *Minority Report*. The punch card-based system was discontinued, but now technologies like scanners, barcodes and loyalty cards provide an alternate means of control.

Gerdes Jr., J.H., Kalvenes, J., & Huang, C. (2009). Multi-dimensional credentialing using veiled certificates: Protecting privacy in the face of regulatory reporting requirements. *Computer & Security*, 28, 248–259.

This technical paper introduces the privacy protective concept of the veiled certificate, which is a type of digital certificate compatible with X.509 standards. Veiled certificates address the ongoing privacy problem of people losing control over their personal identifiers when they disclose them to third parties. A personal identifier is defined here as a number capable of uniquely identifying a person, e.g. social security number. Veiled certificates essentially eliminate unapproved database cross-linking, reducing chances of identity theft. Other types of digital certificates, e.g. blind and user-centric, are also discussed. A helpful table that lays out the properties of different types of traditional and digital certificates is provided on page 254. Veiled certificates are similar to anonymous credentials and zero-knowledge proofs like U-Prove. They also enable users to authenticate themselves without having to actually hand over personal information, e.g. date of birth, to a third party.

Godoe, H. and Hansen T.B. (2009). Technological regimes in m-commerce: Convergence as a barrier to diffusion and entrepreneurship? *Telecommunications Policy*. 33, 19–28.

The authors make the argument that mobile commerce (m-commerce) has thus far failed to become popular outside of Asia largely because of weak government regulatory policy. They compare the fledgling m-commerce industry to the dot-com boom, and suggest that many of the projects from that boom were successful because they fit easily into the libertarian, free market ideology of the time. But m-commerce cannot thrive under such ideology because it needs more government regulation in order to succeed. Specifically, it needs a regulatory hand guiding the fragmentation in the market toward some kind of unity. The banks, telcos, handset manufacturers, etc. need to more properly “converge” if m-commerce is ever going to take off. GSM-based SMS in Europe and iMode in Japan, for instance, required government-initiated cooperative institutions in order to develop into successful technologies.

Gosselin, S. (2011). QR Codes vs. Near Field Communications: Do you need to choose? Retrieved on April 26, 2011.

[HTTP://VESTADVERTISING.COM/BLOG/QR-CODES-VS-NEAR-FIELD-COMMUNICATIONS-DO-YOU-NEED-TO-CHOOSE/](http://vestadvertising.com/blog/qr-codes-vs-near-field-communications-do-you-need-to-choose/)

This article makes the argument that there will be a place in the smartphone market for both QR codes and NFC. Various sources have been claiming that NFC will make QR codes obsolete. Brief definitions of QR and NFC are provided in layman’s terms. The key difference is that an NFC chip must be embedded in or attached to a phone, whereas a QR code only requires a QR reader app. Gosselin says that NFC has significant advantages over QR, e.g. it scans quicker and can perform more complex functions. But QR codes are cheaper and easier to disseminate. This analysis is helpful because the emerging digital wallet technologies tend to be built around either QR or NFC. It will be helpful to consider the pros/cons of each approach and where Prop-ID can contribute.

Gurses, S. (2010). PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. *Identity in the Information Society*, 3, 539–63.

This paper points out the limitations in conceiving of privacy from a techno-centric (computer science) or human-centric (social science) perspective. Gurses argues that more of a balance between the two perspectives is required in the development of PETs. She says, “technical solutions should be used to protect privacy instead of relying solely on legal measures.” This is an argument in support of Prop-ID. Secondary use (p. 544) and chilling effect (p. 547) are discussed. The notion of customer agency is discussed, arguing that each customer should “be enabled in (co)-authoring their own identity.” The paper calls attention to an oncoming “battle over meaning” as surveillance proliferates and the “multiplicity of selves will be distorted and exploited by the consumer-corporate system.” But it is emphasized that customers must remain engaged in the surveillance space rather than withdraw from it. Rather than shutting users out of this space as the simple “right to be let alone” conception of privacy advocates, Prop-ID will allow users to participate and negotiate in this surveillance space more democratically.

Halperin, R. & Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the Information Society*, 1, 71–87.

This paper provides recommendations on how to approach identity-related research. It says one important question to address is: “What are the tools (technical solutions) that can be used to support the management of identity and identification?” Prop-ID is certainly one of these tools. The EU’s Lisbon Strategy emphasized that building trust is one of the key principles that should guide eID development, also a key Prop-ID goal. It addresses government (p. 78) and business (p. 79) applications of ID systems separately. Good line: “We conclude that the rapid take-up of identity management systems in many application areas sends us the message of how central they are to the emerging information society.”

Hodel-Widmer, T.B. (2006). Designing databases that enhance people’s privacy without hindering organizations. *Ethics and Information Technology*, 8(3), 3–15.

This paper uses the notion of informational self-determination to argue that database systems should become more transparent and participatory. It lays out six “newly interpreted principles” for the responsible management of private information (p. 8). The notion of informational privacy is also explored (p. 6). This should be of use to Prop-ID in articulating exactly what we mean by these concepts. Auditing is discussed, p. 9. The technical term “purpose specification” is used to refer to the idea that a user should be able to specify how their data are used.

Hornung, G. and Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self determination. *Computer Law & Security Review*, 25, 84–88.

This short paper outlines the German legal doctrine of informational self-determination. This concept was enshrined in German law in the 1980s after citizens took issue with a required population census. This concept is especially useful to the Prop-ID project because it allows us to determine exactly what we mean by “privacy”. The Prop-ID concept of privacy is close to the German notion of informational self-determination, which states that privacy is about allowing an individual to protect the consistency of their identity. It is about allowing people to have better control over the development of their personality. It is not merely about “the right to be let alone,” as Brandeis would say. The paper uses the term “personality profiles” to describe the precarious results of unchecked data collection practices.

Karyda, M., Gritzalis, S., Park, J.H. & Kokolakis, S. (2009). Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. *Internet Research*, 19(2), 194–208.

The paper opens with useful distinctions between ubiquitous computing (ubicomp) and ambient intelligence (Aml). The authors argue that privacy protection is important not just for individuals but for society as a whole because it is critical for proper democratic engagement. Beckwith's privacy diamond is cited in order to encourage thinking about the interaction between the device, the individual and the information system(s) in ubicomp environments. Providing user notification and awareness in ubicomp environments is especially difficult because the underlying information processing is usually invisible. The authors stress the importance of designing user-friendly interfaces to allow better communication. The term asymmetry of power is used to describe situations in which users employ privacy-enhancing technology, only to find out that the use of this technology is unfairly excluding them from certain services. The authors end by pointing out the contradiction between an individualistic approach to privacy that leaves it up to users to protect their information and a social approach to privacy that makes it more of a collective issue. They argue that this individual vs social responsibility dilemma must be resolved before effective technical advancement can take place.

King, N.J. and Jessen, P.W. (2010a). Profiling the mobile customer - Privacy concerns when behavioural advertisers target mobile phones - Part I. *Computer Law & Security Review*, 26, 455–478.

This article surveys privacy policy with regard to the mobile phone industry in the EU and US. The EU policies are generally more all-encompassing and do a better job of imposing limits on how companies can conduct consumer profiling than the US policies. But shortcomings in the EU policies are also discussed. Details about consumer profiling practices in the mobile space are provided, e.g. how companies are now combining both online and offline data to generate profiles and classify consumers. Specific examples regarding how consumer profiling can be problematic are also provided, e.g. inducing addicts to keep gambling or smoking. It is suggested that if consumers can gain access to these "knowledge profiles" and find out why/how they are being classified in a particular way, they may be motivated to react against profiling. The Council of Europe's 2010 draft recommendation advises member states to develop privacy-enhancing technologies (PETs) that enable mobile users to permit or reject consumer profiling. Our Prop-ID mobile app can be considered one of these PETs.

King, N.J. and Jessen, P.W. (2010b). Profiling the mobile customer - Is industry self-regulation adequate to protect consumer privacy when behavioural advertisers target mobile phones? - Part II. *Computer Law & Security Review*, 26, 595–612.

After describing the privacy concerns faced by mobile consumers in Part I, Part II looks more specifically at what can be done in the industry to better serve the public interest. The authors suggest that relying on the mobile industry to self-regulate is not sufficient and legislative reform is necessary. PETs are compared with transparency-enhancing technologies (TETs) and the authors suggest that more work needs to be done on developing TETs. They point out flaws in the leading industry self-regulatory codes in the EU and US. The codes do not prevent the creation of profiles on groups who are especially vulnerable to consumer profiling, e.g. consumers who have disabilities, consumers who are addicts, etc. The authors discuss the ongoing debate over how to define "sensitive data." Profiles applied to mobile customers are likely to be more personalized and localized because of the private nature of the device. Mobile consumer profiling, therefore, can be very powerful and potentially damaging if left unregulated.

Krumm, J. (2011). Ubiquitous Advertising: The Killer Application for the 21st Century. *Pervasive Computing*, p. 66–73.

This article discusses how advertising business models will increasingly be tied into the development of ubiquitous computing applications in years to come. The mobile phone is mentioned specifically as a ubicomp platform that is particularly interesting to advertisers; about half the world's population owns one now. Krumm explains the consumer profiling practiced by advertisers using loyalty cards, location details and other types of data. This practice is called "segmentation and targeting." A particular type of segmentation is called VALS (Values and Lifestyles), in which consumers are categorized based on their inferred psychological traits. A case study that shows the various ubicomp advertising practices that one can face in the near future is provided. E.g. an RFID sensor on one's mobile phone detects that they just purchased food. A different, perhaps more expensive brand is then recommended to the person based on consumer profiling. The privacy implications of the ongoing development of ubiquitous advertising are clear and Prop-ID could contribute toward inserting more nuanced awareness and discourse about privacy into this space.

Kwang, K. (2011). Swift mobile wallet adoption hinges on apps. Retrieved on April 30, 2011.

[HTTP://WWW.ZDNETASIA.COM/SWIFT-MOBILE-WALLET-ADOPTION-HINGES-ON-APPS-62208623.HTM](http://www.zdnetasia.com/swift-mobile-wallet-adoption-hinges-on-apps-62208623.htm)

The article explains that the release of NFC standards means that the NFC interoperability problem has largely been solved and it is now up to innovative app developers to generate consumer demand and push the mobile wallet market forward. The moves that major players Google and Nokia have been making into NFC handset territory signify the oncoming popularity of mobile wallets. One study predicted that NFC-enabled smartphones will comprise almost 30% of all smartphone sales by 2015. Tagawa, chairman of the NFC Forum, encourages developers to start mapping out use cases for NFC-enabled mobile phones in order to foster demand.

Le Metayer, D. and Monteleone, S. (2009). Automated consent through privacy agents: Legal requirements and technical architecture. *Computer Law and Security Review*, 25, 136–144.

This paper proposes a software architecture called Privacy Agents in which the software would automatically make privacy decisions for the user. The rationale behind this is that the traditional notion of "informed consent" cannot be upheld in today's society with the constant proliferation of technologies that use personal information. By always directly asking the user if he consents before his personal information is disseminated, the user will eventually give up and passively consent. This is especially true in light of mobile phones, where users are even less willing to look at privacy policies on tiny screens. The Privacy Agent would act as a surrogate for the user and manage personal information on his behalf. The user would initially define his own "disclosure policy" that explains what he is willing to disseminate in various contexts. The policy would be defined in a restricted language called SIMPL (SIMple Privacy Language). The privacy-related actions would be logged in the software by Auditor Agents to provide verification. The Prop-ID project shares the goal of selective disclosure with Privacy Agents but we haven't considered a fully automated application. It would be interesting to consider if we could learn from Privacy Agents at all to perhaps make our prototype more automated.

Mallat, N. & Tuunainen, V.K. (2008). Exploring Merchant Adoption of Mobile Payment Systems: An Empirical Study. *e-Service Journal*, 6(2), 24–57.

The paper provides a qualitative and quantitative analysis of merchant adoption of mobile payments system in Finland, which has long been one of the leading markets for mobile devices and services. Three different mobile transaction contexts are discussed – mobile commerce, remote commerce and point-of-sale. The

authors describe various barriers to the adoption of mobile payments identified by retailers, e.g. cost, non-usage, lack of trust, lack of standardization. Prerequisites to the adoption of mobile payments are identified, e.g. the need for a viable payment infrastructure. Retailer benefits to m-commerce are also described, e.g. increased impulse purchases, positive effect on company image. A research framework (p. 48) is provided for future study of mobile payment systems. This is useful to Prop-ID in that the paper can be used to show the issues that need to be overcome on the retailer side of m-commerce. Prop-ID will fulfill the benefit of “positive effect on company image” but for reasons not identified in the paper. Rather than merely making the retailer appear innovative, Prop-ID will show that the retailer values their customers’ privacy. Research question: can Prop-ID also be used to enhance trust in start-up mobile payment providers?

Martin, Z. (2011). The mobile as a credential. Retrieved on May 2, 2011.

[HTTP://WWW.NFCNEWS.COM/2011/06/07/THE-MOBILE-AS-A-CREDENTIAL](http://www.nfcnews.com/2011/06/07/the-mobile-as-a-credential)

This cover story for re:ID Magazine provides a balanced overview of current industry discourse about digital wallets. Telcos, phone manufacturers and payment processors are all suddenly jumping on the NFC bandwagon but, as Martin notes, trust between consumers and industry regarding digital wallets has yet to be established. The article looks at some of the technical issues behind developing digital wallets, e.g. authentication. Martin notes that additional access controls must be put in place for digital wallets; PIN is no longer sufficient. The man-in-the-middle attacks common with mobile technology could be mitigated by PKI, but many industry experts believe that mobile phones cannot properly handle PKI. Most SIM cards, for instance, do not have the capability to store a PKI app. Some say a better alternative for authentication would be microSD cards because telcos aren’t involved in their issuance and that gives the industry greater freedom to rollout a new technology. Most companies, such as RSA, are not focusing on identity credentials for digital wallets. Instead, industry seems more focused on handling the payment potential first. The report ultimately predicts that “payments will be the first NFC app and identity will come later,” within 2-4 years.

Manzerolle, V. & Smeltzer, S. (2011). Consumer Databases and the Commercial Mediation of Identity. *Surveillance & Society*, 8(3), 323–37.

This paper uses database aggregation practices as an explanation for many of the failings of neoliberal ideology. For instance, the US subprime mortgage crisis is linked by the writers to “informational asymmetries that stem from the commercial use of consumer databases.” Consumer debt is exacerbated largely because of commercial entities that – based on aggregated data profiles – convince citizens to make purchasing decisions they can’t afford. Prop-ID would encourage citizens to be more reflective and selective about their personal information and, therefore, lead to an economically stabler populace. The company Acxiom is used as an example of how data collection authorities have been reifying power imbalances and creating societal problems. The paper argues convincingly that “the state should take a more active role in protecting the privacy of citizens.”

Michelfelder, D.P. (2010). Philosophy, Privacy, and Pervasive Computing. *AI & Society*, 25, 61–70.

The paper discusses the privacy issues associated with the rise of pervasive computing, of which Internet-enabled mobile phones will play a significant role. Michelfelder reinforces the position held by Nissenbaum and other scholars that the distinction between what does and does not count as personal information needs to be better clarified. Specifically, the concept of personal information should be expanded. Michelfelder uses the term existential autonomy to refer to one’s ability to decide for oneself whether or not to provide personal information. Michelfelder says this will affect not only individual privacy but our ability to relate to others and the public world as well. Michelfelder also mentions Lederer’s framework

for preserving privacy in pervasive computing environments. This framework relates closely to Prop-ID's concept of selective disclosure. It would require users to define different "faces" for particular situations, and stipulate what information can or cannot be collected.

Mobio. (n.d.). Mobio – Empowering Identity. Retrieved February 23, 2011.

[HTTP://WWW.MOBIOID.COM/](http://www.mobioid.com/)

Mobio is a smartphone application available for the iPhone and Android. The app seems very similar to the Prop-ID project. A key difference is that Mobio uses barcodes and QR codes rather than NFC. But Mobio is about more than facilitating transactions between customers and companies. It states on its website that it is also very much about helping people to retain control over their identity. It states, "your identity is your most valuable asset and we know how difficult it has become to understand how your identity information is actually being used by third parties." The Prop-ID prototype smartphone app will also enable users to perform identity negotiation with merchants.

Morawczynski, O. and Miscione, G. (2008). Examining trust in mobile banking transactions: the case of M-PESA in Kenya. In C. Avgerou, M.L. Smith and P. Besselaar (Eds.), IFIP International Federation for Information Processing, 282, 287–298.

This paper explores the notion that the establishment of trust is crucial for the acceptance of a mobile payment system. It looks specifically at the success of the mobile payment system M-PESA in Kenya. The authors suggest that a major reason why M-PESA was accepted so readily by Kenyans was because of their well-established trust in Safaricom, the telco company behind the project. The authors stress the difference between interpersonal trust and institutional trust. The M-PESA system has shown signs of breakdown where interpersonal trust has weakened, e.g. customers arguing with merchants over technical problems. But the institutional trust between the customers and Safaricom has long remained strong, allowing the system to survive. The authors encourage future researchers to examine this notion of "brand trust" in the deployment of mobile payment systems elsewhere. It is suggested that Safaricom's brand trust was established largely because of the respected image of its president, Michael Joseph. How will Western companies gain a similar level of trust with customers when attempting to deploy mobile payment systems? The Prop-ID project could certainly help companies to establish this much-needed trust factor in the deployment of mobile payment/identity systems by helping them to show that they take privacy seriously.

Mydex. (n.d.). Mydex. Retrieved February 23, 2011. [HTTP://MYDEX.ORG/](http://mydex.org/)

Mydex is a Community Interest Company that provides individuals with Personal Data Stores "to control what information they share with which people and organisations, [and] when." Mydex works on smartphones and PCs. This project shares the same core principles as Prop-ID – restructuring power imbalances, empowering individuals, enabling selective disclosure, etc. but seems to be geared toward online rather than offline transactions.

Nissenbaum, H. (2004). Technology, Values, and the Justice System: Privacy and Contextual Integrity, *Washington Law Review*, 79, 119–57.

This paper uses the notion of contextual integrity as a benchmark for determining whether or not privacy has been violated in a particular situation. Contextual integrity encompasses two types of informational norms: appropriateness and distribution. "The notion that when individuals venture out in public—a street, a square, a park, a market, a football game—no norms are in operation, that 'anything goes,' is pure fiction," Nissenbaum writes. This is relevant to Prop-ID in that we should attempt to explicate the norms of

appropriateness for each setting that we examine, e.g. a bar vs. a post office. Norms of distribution refer to the flows of information between entities. These norms are often more difficult to ascertain and not necessarily moral. Prop-ID, therefore, should not only investigate both types of norms but also consider prescriptive ideas, e.g. what the norms should be in each given context.

OECD Directorate for Science, Technology and Industry. (2007). At a Crossroads: Personhood and Digital Identity in the Information Society. OECD Working Paper series. 1-54. DOC file.

This paper provides a thorough overview of the concept of identity management (IDM) and explains why it will be of utmost importance as new technologies emerge in the information economy. It looks at the philosophical origins of privacy law. The European data protection laws are influenced by the communitarian ideas of Hegel, whereas the US privacy laws are more influenced by the individualism of Locke. The paper points out that when identity information becomes detached from a person's control, that person's participation in society can be diminished. This harms the development of a person's sense of self – their "personhood." This problem is exacerbated when people are denied access to their "identity dossier." The paper identifies decentralization and selective disclosure as qualities that will come into demand as technologies continue to proliferate. There will be a growth in demand for user control as privacy concerns are made more apparent. Nine "properties of identity" that privacy legislation should adhere to are laid out, including the notion that identity is contextual. Good explanations of single sign-on (SSO) and federation are also provided. The paper makes a distinction between user-centric identity systems and federated identity systems, arguing that federated systems are biased against the user because only relying parties can make decisions. The 1980 OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data are provided at the end of the paper. Particularly relevant to Prop-ID is the Use Limitation Principle.

Office of the Privacy Commissioner of Canada. (2008). Backgrounder – Ticketmaster Investigation. Retrieved on February 12, 2011. [HTTP://WWW.PRIV.GC.CA/CF-DC/2008/BG_20080212_E.CFM](http://www.priv.gc.ca/CF-DC/2008/BG_20080212_E.CFM)

Here is a Canadian example of PIPEDA violations by a company, Ticketmaster, found on the OPC's website. It does not involve physical cards but still relates to Prop-ID in principle. The personal information was provided online and then transferred to third parties for marketing purposes without the customer's consent. This highlights the problem of secondary use that Solove writes about. The OPC specifically states: "marketing is a secondary use, and, as such, requires fully informed customer consent (i.e., an opt-in option) or an opportunity to opt out without being penalized."

Office of the Privacy Commissioner of Canada. (2008). Identification machines and video cameras in bars examined. Retrieved on February 17, 2011. [HTTP://WWW.PRIV.GC.CA/CF-DC/2008/396_20080227_E.CFM](http://www.priv.gc.ca/CF-DC/2008/396_20080227_E.CFM)

Canad Inns based in Manitoba committed a number of PIPEDA violations. Especially relevant to Prop-ID is the fact that the company used a card reader to collect a bar patron's driver's license information without forewarning her about this practice. OPC determined that the company's stated purposes for the data collection (age verification, security) were inadequate. OPC recommended that Canad Inns stop recording personal information and dispose of all collected information in its database, but Canad Inns refused. The case is therefore partially unresolved. Misconceptions to knock down: "police services were of the view that such measures encourage customer accountability and improve safety."

Office of the Privacy Commissioner of Canada. (2009). Fraud detection not an acceptable reason to collect driver's licence numbers for store memberships. Retrieved on March 19, 2011.

[HTTP://WWW.PRIV.GC.CA/CF-DC/2009/2009_014_0529_E.CFM](http://www.priv.gc.ca/CF-DC/2009/2009_014_0529_E.CFM)

When an individual provided her driver's license for membership at a store, her license number and full date of birth were recorded by the store and held within its database. The store did not provide a reason for this retention of personal information. When the customer requested a copy of her personal information, the store was unresponsive. The OPC then investigated the matter and found that the store was in violation of multiple PIPEDA principles. Namely, a unique identifier such as a driver's license number is not required for fraud detection or conducting a credit check. Credit reporting agencies only need one's name and address. This case represents the kind of problematic lack of communication between customer and retailer that the Prop-ID project wishes to ameliorate.

Palmer, D., Warren, I. and Miller, P. (2010). ID scanners in the night time economy, in Michael, Katina (eds), ISTAS 2010: Proceedings of the IEEE International Symposium on Technology and Society: Social Implications of Emerging Technologies, 234–241.

This paper takes a critical look at the emerging practice of ID swiping in the city of Geelong, Australia. The authors conducted an empirical study, interviewing patrons and club owners about their perspectives on ID swiping. Most stakeholders were very optimistic about ID scanning and seemed dismissive of the potential drawbacks, e.g. privacy concerns. The authors use Haggerty & Ericson's concept of the surveillant assemblage to illustrate how data captured in the specific context of a nightclub can be abstracted from that setting and reassembled with other kinds of data, unbeknownst to the patron. The authors note that when police begin to rely on such technologies, they are essentially "policing through the lens" rather than through interpersonal communication. This ultimately disconnects police from their communities, and vice versa. The authors found that the direct impact of reducing violence through ID swiping was minimal in the Geelong area. Like CCTV, the authors argue, ID swiping merely displaces undesirable behaviour.

Patten, G. (2010). Guilt by Association: Canada, Identity Cards and the Myth of Privacy. Unpublished, 1–17. [HTTP://WWW.GRPATTEN.COM/POLICY/GUILT.PDF](http://www.grpatten.com/policy/guilt.pdf)

This paper provides a nice complement to the Solove and Nissenbaum papers. It relates their ideas specifically to identity cards. Patten explains why aggregation and exclusion are important issues re: identity cards and uses the compelling example of Alistair Butt, a 10-year-old placed inexplicably on the no-fly list. Patten shows how mass aggregation and interpretation of data without public input results in the reification and simplification of classifications that could potentially hurt one's life chances. These are important issues to reinforce in the Prop-ID project.

Perez, S. (2011). NFC in 2011: Who's building your mobile wallet? Retrieved on April 24, 2011.

[HTTP://WWW.READWRITEWEB.COM/MOBILE/2011/03/NFC-IN-2011-WHOS-BUILDING-YOUR-MOBILE-WALLET.PHP](http://www.readwriteweb.com/mobile/2011/03/nfc-in-2011-whos-building-your-mobile-wallet.php)

This article provides an overview of the key stakeholders in the burgeoning mobile wallet field: mobile platform providers, telecommunications operators and banks. The article begins with a definition of mobile wallet, explaining that the term refers not just to an app but also to the secure element on the phone. Platform providers like Apple and Google are interested in using the secure element embedded in each phone to store and authenticate personal information. But telcos like China Unicom and Telenor are interested in using a SIM card instead so that the providers do not retain complete control over the system. Certain banks, such as Bank of America and Wells Fargo, have also been deploying mobile wallet solutions on their own. These solutions usually involve an NFC-enabled microSD card that can be inserted into a phone's memory slot.

Rauhofer, J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society. *Information & Communications Technology Law*, 17(3), 185–197.

This paper explores the idea that the market value of privacy has declined in recent years to become something of a non-entity. People are continually coaxed into disclosing more and more information about themselves. They are persuaded by organizations that the benefits of disclosing this information outweigh the risks. The Brandeis concept of privacy as “the right to be let alone” is discussed. Rauhofer ultimately argues that this is an overly narrow conception of privacy because it privileges individual over community values. Privacy should be conceived as having public, communitarian value that is necessary for equal participation in a democratic society. The term “data havens” is used to describe countries with few or no data protection laws. Risk profiling systems are discussed. If left unchecked, rampant risk profiling will evolve into social categorizing that unfairly privileges certain segments of the population over others.

Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27, 45–52.

This article provides an introduction to the practice of data mining and an overview of the risks associated with it. Schermer identifies three negative consequences of data mining: discrimination, de-individualisation and information asymmetries. In de-individualisation, people are judged on the basis of their inclusion in a group rather than as individuals. This can lead to unfair stigmatisation. The concept of data dredging is also discussed, in which what might be true only for a particular data set is inappropriately associated with a larger data set. Schermer is critical of the concept of data minimisation. He says it does not necessarily protect against the risks of profiling and might actually strengthen unfair profiling by rendering the detection of discrimination more difficult. He says that traditional *ex ante* privacy protection is insufficient and more attention must be paid to developing *ex post* accountability. The Prop-ID project takes essentially an *a priori, ex ante* approach to privacy protection by encouraging data minimisation before the event of profiling. This paper will be helpful in getting us to think critically about the value of our approach and address the arguments about its ineffectiveness.

Shilton, K. (2010). Participatory Sensing: Building Empowering Surveillance. *Surveillance & Society*, 8(2), 131–50.

This paper puts forth the idea of participatory sensing (PS) as a means of providing individuals with “the capacity to answer back.” Using mobile phones, people can collect and aggregate their own data. This will allow people to make an alternate case to corporations/governments that have engaged in data collection about them. The aggregated data can feed into a Personal Data Vault (PDV), which could “encourage selective sharing by helping individuals broker data sharing arrangements with multiple service providers.” This project would enhance data literacy by encouraging people to reflect on how meaning is ascribed to their activities by data collection authorities. This broadly relates to Prop-ID in that the goal of PS is essentially the same – to challenge the data aggregation power structures of the status quo and give everyday citizens more agency within surveillance mechanisms. The idea of a PDV could also likely be tied into Prop-ID.

Solove, D.J. (2007). ‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy. *San Diego Law Review*, 44, 745–72.

This paper represents the most nuanced conception of privacy that we have encountered. The Prop-ID project should utilize Solove’s explanations in helping people to understand why privacy should be a concern for everyone, even if you think you have nothing to hide. Ann Cavoukian and much of the PbD literature holds that privacy is “the right to be let alone,” but Solove argues convincingly that this is an overly

simplistic conceptualization. Solove provides a number of specific examples of privacy violations, such as *Dyer v. Northwest Airlines*. This case illustrates that “there is a social value in ensuring that companies adhere to established limits on the way they use personal information. Otherwise, any stated limits become meaningless, and companies have discretion to boundlessly use data.”

Stalder, F. (2002). Privacy is not the antidote to surveillance. *Surveillance & Society*, 1(1), 120–24.

This short article clearly explains privacy issues in layman’s terms. Stalder echoes Solove’s opinion that the widespread conception of privacy as a personal issue – the “bubble theory of privacy” – is problematic. Stalder specifically mentions marketing as a problem area. He recognizes that in order to confront these issues properly, we cannot simply close ourselves off to surveillance; we need to engage with it. Stalder says the cognitive load is too high for people to make complex decisions about data collection. Perhaps Prop-ID could reduce this cognitive load. This article should be useful to Prop-ID in breaking down misconceptions about privacy issues.

Stoddart, E. (2008). Who watches the watchers? Towards an ethic of surveillance in a digital age. *Studies in Christian Ethics*, 21(3), 362–381.

Although Prop-ID is a secular academic project, this paper illustrates concepts behind Christian social teaching that fit well with the Prop-ID project. Namely, the concept of subsidiarity is stressed. Stoddart argues that human dignity is best preserved when control over surveillance is localized and put in the hands of citizens. Centralizing initiatives that push decisionmaking into higher realms of power need to be clearly justified. Prop-ID, similarly, is all about allowing surveillance decisions to be made locally by the citizens themselves. But Stoddart stresses that subsidiarity must be considered in tandem with solidarity; otherwise, we devolve into mere individualism. This is the notion that we should all feel a mutual responsibility for one another’s “data image” because of our inherent interconnectedness. Subsidiarity and solidarity are about more than mere individualism, then. They are about the common good. Stoddart notes that the threat of databases exists in the “multiplication of the individual” to the point of a loss of control. Surveillance technologies excessively focus on pre-emption, instilling in groups of people a harmful “categorical suspicion.” Stoddart recommends that we focus more on preventative measures to address the systemic issues, e.g. poverty, racism, religious hatred.

Swilley, E. (2010). Technology rejection: the case of the wallet phone. *Journal of Consumer Marketing*, 27(4), 304–312.

Based on empirical research, this paper presents a somewhat pessimistic view of wallet phone technology. Two groups were studied for this project – young college students and a more generalized population. They were asked about their attitudes toward the idea of a wallet phone. The technology acceptance model (TAM) was applied to generate a number of hypotheses regarding wallet phones. (p. 305) The concepts of perceived risk, security/privacy, innovation resistance and resistance to change were all applied to this analysis. To sum up: “in both studies, not only did the respondents not like the idea of a wallet phone, they do not intend to use a wallet phone.” Swilley does provide some room for optimism, however. She writes, “as with many other technologies, such as microwave ovens (Kasulis et al., 1979), it may be that consumers do not understand the need for such technology, as they are satisfied with the cell phone technology.” Prop-ID, then, should use this study to acknowledge the reservations consumers have about wallet phones and attempt to address those concerns. Swilley also advises that wallet phone developers spend time articulating a specific target market because “it is obviously not for the general public, as of yet.”

Taylor, J.A., Lips, M. & Organ, J. (2008). Identification practices in government: citizen surveillance and the quest for public service improvement. *Identity in the Information Society*, 1, 135–54.

This paper focuses particularly on public sector surveillance issues. It attempts to reconcile the two competing perspectives of the 'service state' vs. the 'surveillance state'. The service state is the beneficial conception of surveillance – providing essential services. The surveillance state is the more negative viewpoint, holding that surveillance is invasive in harmful ways. Of particular interest to Prop-ID is that the paper uses a driver's license case study to illustrate the misuse of personal information when it is transferred to third parties. The paper also uses Nissenbaum's concept of contextual integrity to deliver the point that informational flows/norms of distribution need to be negotiated between citizens and government more appropriately. Privacy audits, social sorting, function creep and data sharing are also discussed.

University of Freiburg. (n.d.). Online-Demonstration des ID-Managers. Retrieved February 22, 2011.

[HTTP://WWW.IIG.UNI-FREIBURG.DE/TELEMATIK/AT05/IDM-DEMO/](http://www.iig.uni-freiburg.de/telematik/at05/idm-demo/)

This webpage provides an interactive online demo of the iManager application. It is in German. This could perhaps be of use in designing a privacy-protective smartphone application.

Wladawsky-Berger, I. (2011). The evolution of money. Retrieved on April 26, 2011.

[HTTP://IDEAS.ECONOMIST.COM/BLOG/EVOLUTION-MONEY](http://ideas.economist.com/blog/evolution-money)

The author predicts that 'smart digital wallets' will be disruptive technologies that transform the global financial landscape. He compares digital wallets to browsers, noting that browsers became the standard technology for accessing the internet. Similarly, he claims, digital wallets will become the standard for accessing money. He takes a very optimistic view of digital wallet technology by claiming that it will also lead to enhanced universal inclusiveness. Many people in developing countries do not have bank accounts, but they do have mobile phones. The idea is that digital wallets will enable these hitherto excluded people to more fully engage with the world economy. He notes that the public sector should have a significant role to play in the development of digital wallets because of its existing involvement in the regulation of financial and identity transactions.