## Notes for Dissertation

The possible outcomes of this simulation are broad and encompass the following;

1. Education alone is not sufficient to promote safe privacy preserving user behaviour
2. Education need to be extensive, pervasive and enduring to have a desired effect
3. Over time education may succeed, even though modest.
4. High privacy education could obsolete low privacy engineered systems
5. The advantages of Privacy engineering are greater that education

### My Personal Objectives

1. To further my understanding of user sensitivities around disclosure, privacy and trust;
2. To further my complex system simulation development
3. To do something interesting

### Research Material to Consider

1. Zero knowledge protocols
2. Privacy by design
3. Social Engineering Attacks
4. Popularity Correlated Trust
5. Privacy Education (Pedagogy)
6. Ambient Intelligence
7. Cyber Game Theory
8. Data Communications Bill
9. Online behavioural Advertising (deep packet inspection)

### Key Words

1. Authentication
2. Privacy
3. Security
4. Cybercrime
5. Identity
6. Signalling Games

Table 1: A non-exhaustive list of interdisciplinary perspectives on privacy on the web

|  |
| --- |
| **Privacy by Design (PbD)** |
| **Law (Regulatory):** milestones in the legal framework for an organisation’s privacy obligations  **Business Ethics:** the mindsets of organisations promoting over disclosure  **Privacy Engineering:** techniques and challenges of implementation  **Politics:** governance and pressure on organisations (security v liberty)  **Social**: reputation and stakeholder management |
| **Privacy Education** |
| **Law (protective):** the legal framework to help compensate and litigate privacy transgressions  **Consumer** **Awareness**: understanding of consequences, threats and rights  **Social** **Engineering**: a system is only as secure as the people using it.  **Politics**: how user engagement and vocalisation is influencing organisation behaviour  **Social:** passive trust and naive actions such as over disclosure in a cyber domain |

TAMI – wish to represent laws in N3

Deductive reasoning using logic – difficult. Probable cause is not mathematical. Contextual integrity.

Efficient supply chain can lead to the transparent customer

Welfare and security -> the police state or even stifled communications (link)

Malicious attacks difference from ID theft and hassle

People will work in smart workplaces first – so priorities there.

As these systems become more prevalent and fall into our unconsciousness it is perhaps more imperative that the academic community maintain if not intensify its scrutiny (Thrift 2004). On the other hand the level of threat and malignant action against these systems maybe a natural by-product of a technological society thus it maybe argued that the sophistication of threat is likely to escalate with the sophistication of protection. Will society be required to actually choose between privacy and security (Bin in Jain et al., 2004) is a technological deterministic force prevailing, is the erosion of privacy is a consequence of an inevitable evolution of technology?

Cryptography = access limitation.

More difficult to restrict also wrong time and new information is created not accessed.

User control laws – difficult – impractical

Non existent legal framework for governed mining of commercial data. CDT report on the Privacy Gap 2003. Privacy preserving data mining – Lindall 2002

HCI cost of privacy

– what happened to the oxygen project? Mit 2000

What is the NIEM Model? National information change model

### National information market

Cost of storage v cost of sorting

## Technological considerations

Ambient tech, data mining, location aware

Inference Techniques

Capabilities

Who does it, why

|  |
| --- |
|  |
| **Key** **Words**: |
| **Summary and Contribution**: |
| **Main** **Critique**: |
| **Citation:** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: |
| **Bullet:** |

|  |
| --- |
|  |
| **Key** **Words**: |
| **Summary and Contribution**: |
| **Main** **Critique**: |
| **Citation:** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: |
| **Bullet:** |

|  |
| --- |
|  |
| **Key** **Words**: |
| **Summary and Contribution**: |
| **Main** **Critique**: |
| **Citation:** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: |
| **Bullet:** |

|  |
| --- |
| **Nudging Privacy: The Behavioral Economics of Personal Information** |
| **Key** **Words**: nude, education, informed choice, privacy trade-off |
| **Summary and Contribution**: how to balance the human need for publicity with the need for privacy (utility)  Same tech expanding date processing capability makes the navigation of the privacy trade-off more problematic.  In practice we seem resigned and unfazed to personal data intrusions  Poor views of the stable preferences for privacy making the trade-off coherent. Participate or not? Privacy difficult to estimate, distortion in the way we value data protection and act on value. Subtle effect thus behavioral inconsistencies.  Incomplete information = low discrimination – assurances of safety heighten discrimination? And professional looking = less data – more formal (link with Posner??  Paternal solution – nudge for informed choice – but who pays? |
| **Main** **Critique**:  Who pays? |
| **Citation: Acquisti, A. 2009. "Nudging Privacy: The Behavioral Economics of Personal Information." Security & Privacy, IEEE 7(6):82-85.** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**:  Not a stable trade-off, my model allows for experiential adaptation to participate or not. |
| **Bullet:** |

|  |
| --- |
| **Privacy, identity and security in ambient intelligence: A scenario analysis** |
| **Key** **Words**: Privacy boarders and dimensions, sensing, privacy |
| **Summary and Contribution**:  Ambient technology will make the interaction /privacy trade off even less explicit, which poses particular challenges for social norms and values (one section)  Ambient tech goes beyond current privacy protecting boarders – blurring boundaries between public and privat e spaces, blurring boundaries between then and now, as data is collected and timeline.  Different Dimensions to privacy (empowerment, dignity, utility, regulatory ) [lessig 2000]  Bohn looks at borders – natural, social and special/temporal  Personalization can be great but consequences as people are bundled into potentially vulnerable targets. Automated search = directed thus less choice, less variation in information, less randomness  Efficient supply chain can lead to the transparent customer  Welfare and security -> the police state or even stifled communications (link)  Malicious attacks difference from ID theft and hassle  People will work in smart workplaces first – so priorities there. |
| **Main** **Critique**: |
| **Citation: Friedewald, Michael, Elena Vildjiounaite, Yves Punie, and David Wright. 2007. "Privacy, identity and security in ambient intelligence: A scenario analysis." Telematics and Informatics 24(1):15-29.** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: |
| **Bullet:** |

|  |
| --- |
| **Why we can’t be bothered to read privacy policies** |
| **Key** **Words**: lemons market, incentive |
| **Summary and Contribution**: conflict between consumers wanting to interact online and manage their private information. These authors suggest there is a lemons market and that equilibrium is unlikely or at best unstable.  Privacy is biggest reason people stay offline and those remaining still hold privacy as number 1 concern (but paradox)  Hope that seal programs would improve things but low adoption (2000) but things are improving, less information collected and chice about what happens to information etc, this study looks at where the market ill end up – future direction. Showing that the market is not efficient in the presence of asymmetric information  Information sharing between vendors in the presence of a strategic context leads to a rivacy protecting regime  Read akerlof’s lemon market. About asymmetric information.  Real Networks suffered public criticism when its software was found and reported to gather and give. But this is rare and incentive is low to avoid violating policy. There is no pile up of bodies so law is slow to react and public emotions disengaged.  Testing sites like getting a mechanic to look at a car before you by it. Expensive but risk averse.  Suggest that as all firms respect, customers will stop testing, then as customers stop testing, firms will defect. Cycle! Needs an open and transparent environment. There is a NE but it is unstable. There is overshoot and oscillations. The NE can also change.  Making consumers more aware, cant make an efficient market. It can help but is not sufficient. |
| **Main** **Critique**: |
| **Citation: Vila, Tony, Rachel Greenstadt, and David Molnar. 2003. "Why we can't be bothered to read privacy policies models of privacy economics as a lemons market." Pp. 403-07 in Proceedings of the 5th international conference on Electronic commerce: ACM.** |
| **Impact Factor**:  **Article Citations: 49** |
| **Related to Identity Authentication**:  No privacy comparison website – the choice of vendor comes first the privacy concern, part of the cost is repeating the search…  Consumer awareness is necessary but not sufficient for an efficient market. Need to provide firms with a direct incentive to respect personal information. Enforced laws or reduce consumer testing. The government doing the testing themselves etc. |
| **Bullet:** |

|  |
| --- |
| **Fusion of ID across real and cyber domains** |
| **Key** **Words**: super identity, cyber |
| **Summary and Contribution**:  Looking at tech impact on privacy, security and detection of threat. To provide intelligence and law enforcement agencies with a greatly enhanced ability to identify individuals across real an cyber domains. SID is a multidisciplinary project, technical and behavioral links.  Trying to find the minimal amount of information required instead of a grab all process.  Under benign and malign circumstances people now manage a spectrum of IDs. We believe they all track back to one superID [ thus a combinatorial model will support robust authentication or identification decisions – with confidence indexed by trust in data provenance and the diagnosticity of Id factors being used.  Underreported crime (fraud) but estimated to cost 2£b yearly  We define ID an a concept that distinguishes one individual from another – who you are. ID is quite fluid so perhaps better – who you are NOW. In instance, circumstance and time.  System must recognize that different IDs belong to the same person. A person may occupy a number of real but different roles which is an accurate reflection of an aspect of themselves this maybe quite different in name, behavior, social group etc (dad, CEO)  Partial ID, allows fragments of ID to be amalgamated to verify ID,, whilst maintaining minimal disclosure and maybe increased user trust.  Sullivan (2011) our ID can exist in numerous places and by used in a rapidly increasing set of purposes from national databases to commerce, social comms – Digital id can be used as a commodity to buy services, access information in a way that currency has been used in the past. Broad base to distribute ID but also a broader threat base.  “ a complete sense of ID requires acknowledgement and understanding of the digital or cyber and well as real work context”  security tokens carry a cost to user in terms of retention and fraudulent use of token.  Concept of digital ID now also include cyber metrics – online browsing behavior, memberships, styles of interaction etc how we represent our selves in different forums.  Papers on trust (not privacy) Kinfberg, grimmet, woodgate …2011/09  Who are the European information society?  Combinatorial approach benefits ove single ID measure , but still limited to the established data based of acceptable metrics – thus there is a failure to scale up the techniques. Plus additional computational overheads!  In identification, known information can reduce the search space or tune a classification system to t population sub group.  Still a gap in understanding linkage of real and cyber identity metrics. Especially since the possibility for self-expression is so massive online, but so to is the opportunity for deception.  The monetization of ID is touched upon, but not enough to suggest there will be a moral standpoint and not just the long arm of the law. Although they allude that SID can help ‘keep pace’ with these development, is could be fuel to the flames! |
| **Main** **Critique**: |
| **Citation: black and steveange** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**:  Is different ID belong to the same person and SuperID links them – how to circumvent this.  What is it didn’t matter how ID was collected – just need a confidence on the metric used and a confidence provided by the metric collector. SID tries to priorities metrics, creating a fusion of known measure and a revelation of unknow (inference) along with a confidence.  (current work on creativeity and deception and how we rationalize everyday lies. Also deception is more rife when in the abstract (far from money). Data backs are far from the individual so the moral hazard is introduced.  What are the keystone pieces of ID metrics and can they be destroyed or forbidden? |
| **Bullet:** |

|  |
| --- |
| **The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI** |
| **Key** **Words**: Contextual Integrity, HCI |
| **Summary and Contribution**:  Personal privacy addresses the fluid notion of privacy around a person’s right to control personal information flow  Nissenbaum, views privacy as the appropriated flow of information rather than a static act of sharing. no aspect of human life which is not governed by norms (context specific) of information flow – no universal privacy norms. Social setting can dictate the type of info to be shared (medical) or unspoken code of contact (see Mancini et al) but these norms don’t feature in research on privacy! Ignoring context.  3 principles: protect against government intrusion: restrict access to sensitive info; protect personal space.  Because of digital tech, information can be shared more easily thus new standards for protection are needed.  Sensor based personal tech (location tracking or surveillance) have presented new challenges to an individual’s sense of privacy.  Privacy regulation is not static or rule based, but technologies by definition relies on both of these. How can teach fit into cultural practices of privacy management? “ it appears rather arrow to attempt to generate generalized rule based principles about personal privacy preferences (this is a problem with P3P techniques etc) good link!  Relationships are defined by the type of information shared – intimate – Dr or close friend.  There is a tendency and desire for self-exposure which is a dual pleasure of also being able to snoop on others private lives. ‘feel famous’ when people comment on your information! Suggestion that weak ties dominates online permits this duality best. Also the intention not to share is not a suggestion of being worried they will find out – but other things as irrelevance and modesty are as important as worry.  Identity management online was an ongoing thing with constant monitoring against the social norms of information flow  Social sites – content was self censored to fit the greatest common denominator – MUM. Full of ambiguities and plausible deniability (21 yo drinkers)  May participants were unaware of actual settings – if negative experience = behavior change (not setting changes)  Norms change over time – caller ID  Criticism of prototype tools as a good indication of early findings and behavior but because of lack of lived in situation they merely provide a slice of behavior – need continuous assessment – longitudinal studies.  Need to look up Altman’s theoretical privacy framework (used by palen and dourish)  The word privacy stamps the conception of sensitive data, which is misleading.  Users prefer a manual system where they can control and define the shared data themselves |
| **Main** **Critique**: this paper is a mish mash of muddles privacy concepts – is it location or not?  A suggestion that users want a manual system so they can define the controls is bazaar given the difficulty ot designers to create rules – the cognitive load would be massive and potentially impossible. Better to have a probabilistic system which could learn from ground level actions. |
| **Citation: Barkhuus, Louise. 2012. "The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI." Pp. 367-76 in Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems: ACM.** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**:    Because information can be shared easily with digital the scaling up of previously acknowledged data sharing is not linear. Death by a thousand pin pricks.  Bayesian rule based tech could be a dynamic way forward. P3P has these deficiencies and limitations  Authors recommend avoiding the word privacy as it is muddled and commonly misunderstood – but what, it is a common word which would be said to describe any of it’s replacements. |
| **Bullet:** |

|  |
| --- |
| **Privacy and security of personal information.** |
| **Key** **Words**: economic, markets, online and off lien identity (super ID), technological solutions |
| **Summary and Contribution**: while market forces might ensure fair use of data connected to online ID they do no guarantee optimal use and appropriate protection of off-line ID  Companies dissociating on and off line IS have struggled to to balance the differing need of various parties in the privacy equation, eventually failing to gain widespread adoption.  Privacy is more difficult to sell that protect  Individuals face a trade off between need to reveal and the need to conceal information, 1980 economic view suggesting that left unchecked this tradeoff will find a balance., resulting in the most efficient exchange in personal information . individual and entities interested in the information abut individuals would converge ti that equilibrium regardless of initial allocation of privacy rights.  National information market? Where is it?  Much anecdotal evidence of growing privacy costs and intrusions and reports of scarce adoption and success of privacy technologies offer arguments to al sides. Do individuals act rationally when they chose not o to adopt privacy technologies?  Differentiate between on and off line IDs, same tech to join pieces of information together can be used to spilt them apart? To try and make the re-piecing economically unjustifiable  In general terms when information is freely available market laws alone may produce peareto optimal outcomes. Can make society a better place – targeted service.  There may be economic benefits to sharing and increasing the use of online information  At the peak of the privacy scare 1990s surveys found that ID theft and C card fraud were the main concerns – supporting the view that their are economic incentive to protect ID  Privacy paradox! They discount the potential losses from losing control of their personal information (uncertain but probably large) with the probability that an outcome will take place (uncertain but perceived as low) then compared with the implicit value of using a technology which are certain and immediate – instant gratification.  OFFLINE:  The negative utility coming from a future potential shock is impossible to calculate. Individuals tend for immediate gratification over possible threat.  Hard for techs to survive with low demand and low margins. Except in a niche. Even when tech is cheap adoption of new tech ins not. This lack of privacy tech could be causing a latent market demand untapped.  FTC self regulation has not provide the results expected – because law doesn’t hold them liable to wrong doings! Chase Manhattan v Steve?? See Solove 2004  Con…  Economics needs to be supported by law – (co-design) the costs are preventing the optimal solution – may need to add in Company C! oh dear, could be fun or distracting.  Moral Hazard could be a parameter!!  Economic tools to identify the area of what to share, when and where and legislation to create liabilities replacing the ‘trust me’ model and self regulation. |
| **Main** **Critique**: |
| **Citation: Acquisti, Alessandro. 2004. "Privacy and security of personal information." Pp. 179-86 in Economics of Information Security: Springer.** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**:  Privacy hard to sell than to proect – we have the technology but the economic incentive is not there, so no implementation = not technology demand, stifled innovation.  The same technology which allows for better consumer awareness could be use to evaluate a vunerable target.  At least with ID theft and CC fraud there is a measurable impact on an individual  Incentive to hare and protect, depending on the information.  If individuals are myopic about risks then other parties have little incentive to take the burden. Impliying that withoutout liability for misue or even the acknowledgement of wrongdoing (hard to source) moral hazad ensures. Since the owner who has the burden also has the gratification. |
| **Bullet:** |

|  |
| --- |
| **Ive got nothing to hide…** |
| **Key** **Words**: misunderstandings, surveillance |
| **Summary and Contribution**: an unraveling of the nothing to hide argument for the lack of surveillance resistance.  By saying nothing to hide = I don’t care what happens so long as it doesn’t happen to me”  Talks of Posner’s view that people don’t want quiet, rather the power to conceal.  Differenialst the difference between type of data, - phone numbers v nudity and how likely this information will be captured in government surveillance. Machine collection is more impersonal and he volumn alone suggest there is no invasion of privacy – this is the practical obscurity argument with a twist. (posner)  Suggestion that most people accept survelance as a small exhance for national security gain. However this tradeoff is based on a low valuation of privacy and a relatively high valuation on security so toghether security is a dominant force.  The nothing to hide if formidable – it is difficult for privacy to prevail. The argement suggest that rivacy is about hiding bad things and therfre the argument is already conceded in favour of security.  Privacy is a muddled concept of little use – vague and evanescent “Arther Miller - “infected with pernicious ambiguities” Hyman Gross  Attempts to deifne Privacy have not been met with success! Solove looks at why these past attempts have been so unsatisfying.  Instead of being related by a common denominator, some things share a complicated network of simalirties overlapping and criss crossing sometimes overall simalrities sometimes similarities in detail. Privacy is not reducable to a singular essence.  Survelance and date mining is no the same thing although ofthen banded together by commentators. A distinct difference.  Taxonomy of privacy – Collection;Processing;dissemination;invasion this hit the span of any privacy acrhictechure – look at the work on transparent and accountable data mining (below)  Useful to include the full list with definiations.  There is no one specific criterion for inclusion or exclusion in the rubrix of privacy, violations consist of a web of related related problems without a single common denominator.  Privay can be in conflict with freespeech? But society will genenerally win when balance aginast the needs of an individual, but fails to recognize the societal impact of privacy erosion since most cases are individual led.  A society without privacy would eb suffocating and might not be a place in which most would want to live. When protecting individual rights we as a society decide to hold back in order to receive the benefits of creating free zones for peope to flourish – no longer understand this! – also see posner and the survalance reducing efficiency in a communication market – aka stifiling free speech.  No fourth amendmanet protection when government collects information for others.  Privacy is not he trumpting of the individual against societies interests but the protection of the individual based on societies own norms and values – link to contextual integrity  Privacy’s lack of blood and death or broken bones or buckets of money didtances privacy harms from other catagories of tort law – this connect with the genuine lack of alarmed public and why there is no incentive to change.  Social value in adhere to own policy yet no legal reprisal so stated limits are in effect meaningless and companies have discretion to boundlessly use data. Self regulation is no regulation - business ethics  Court rulesin that no proof of harm (no account for confidentiality breach though) smith v chase manhatttan. Prove loss of time, incinvienence and trust? Weak claims |
| **Main** **Critique**: |
| **Citation:**  Solove, Daniel. 2007. "'I've Got Nothing to Hide'and Other Misunderstandings of Privacy." *San Diego law review* 44. |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: using public security feel to eradicate privacy of society becuas the emotive valuation of security vastly outweights people’s notion of privacy and the nothing to hide!! To seek privacy is to admit the need to hid something. A leading retort    I don’t think privacy will prevail but individuals can benefit from their data resource instead of a third party aggregator.  How many hour between rigby (22nd May) and data bill – 26th May Taresa May? Just a few days before the solution to a terrible event was to increase public survelance.  Need to make a distintio n between the survalaence and the data mining which goes on – prob best to keep it commercial and allude to government.  Can’t put t avalue on privacy as this is a case by case situation, thus many court dismiss it at it is impossible to quaatify or even prove harm.  Also the opt out of individuals from communicating freely or not communicating at all is impractical to measure and therefore difficult to build a case for.  Also data m innig strives to prognosticate about future actions. To what extent – superidentity?  Why is the government exemp from the right to see personal data, |
| **Bullet: Diamond in Closet** |

|  |
| --- |
| **The Economic of Privacy** |
| **Key** **Words**: economics, efficiency, equilibrium |
| **Summary and Contribution**:  3 senses of privacy, Concealment of information, Peace and Quiet, freedom and autonomy  the concealment of information, the target and deemed most interesting from an economic standpoint. can restrict an efficient market (recruitment) thus can restrict financial efficiency in other data markets. Can be considered a form of fraud and there is an asymmetrical spread of cost for the ‘insurance’ of concealment. Cost shifts from one small group to another.  Jusxtaposed the selling of self to the selling of a product. Keeping people in the dark crate inefficiency in the job, marital, friendship etc markets. Talks about t redistribution of weath away from the whites to the racial and ethic group!  Eavesdropping reduces the effectiveness of communication and therefore rasies the cost of unfettered communcation  Information overlaod, used to be costly, but cheaper now – big problem is searhing  There is a rich and growing literature on the economics of information, the same economic factors that determin search behaviour by workers might also determin investments in obtaining and in shielding private information. |
| **Main** **Critique**: |
| **Citation: Posner 1981** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**:  Might have more to do with autonomy and freedom than concealment. But need to mention this Judge, often controversial and outspoken. |
| **Bullet:** |

|  |
| --- |
| **Transparent and Accountable Data Mining** |
| **Key** **Words**: Data Mining, Violations, Antecedents |
| **Summary and Contribution**: this paper looks at a method, which theoretically would ensure a transparent data mining process. Based around the introduction of a TMS, which basically stores the path of data creation. I.e. if A and B was used to generate C. This process would be stored so if C was brought into question there would be acknowledgement to the source.  TMS – store of inferences which led to the new information thus can examine the catalytic piece of information (the Antecedent)  Other aspects regard the use of this information and a mechanism which checks the rules have been followed.  Privacy can’t be controlled by restrictive access since information stored and used in non-permissible ways can be long after the initial collection and therefore long after the violation has occurred against restricted access. Better to restrict use than collection as it is the use, which causes the concern.  Transparent: audit possibility  Accountability: clear acknowledgement of use versus permission – operator makes an informed decision. |
| **Main** **Critique**: although the architecture is simple it fails to work unless the whole system uses it. Where is the incentive to implement this. Would require legal pressure.  “Use” does cause more concern than collect to those used against, however, currently in the big data grab the capability is being built for large-scale surveillance. Same argument as owning a gun and using one. Why allow people to have an arsenal if they cant use it. Eventually they (someone) will.  The same rule of academic plagerism can be appied to personal information. Cite your source. Got a phone call saying I opted into something so I am now receiving a call. With whom did I opt in? how can I find out. If companies really thought we didn’t care they would tell us and allow us to block it. |
| **Citation: Weitzner, Daniel J, Harold Abelson, Tim Berners-Lee, Chris Hanson, James Hendler, Lalana Kagal, Deborah L McGuinness, Gerald Jay Sussman, and K Krasnow Waterman. 2006. "Transparent accountable data mining: New strategies for privacy protection."**  2006 |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: |
| **Bullet:** |

|  |
| --- |
| **Privacy in Context** |
| **Key** **Words**: Co-design space, cost, down stream consequences |
| **Summary and Contribution**:  Co-design space between social, technical and regularity perspectives.  What are the down stream consequences of providing data?  The oxygen project MIT 2001. Data collection explicit or discrete (aware or ignorant)  Argre – privacy Chernobyl 1997 – any third party can access a complete profile of an individual’s daily activity.  Users don’t want to , or can’t control information collection at the sensor level  Care for privacy actually costs HCI (pop ups). HCI interruption of task:  Federal trade commission 2000 guidelines. Most privacy laws and regulations are user centered. These FTC guidelines have No force in law!  Notice: warning of collection and use Choice: Opt out Access: Able to see, amend records Security: Stop unauthorized access  Guidelines did impede law enforcement but not commercial use, which was then resold to law enforcement.  P3P was a platform for privacy preferences which is machine readable, therefore browser side critique of system to inform user.  Or context aware systems which remember last actions and those of trusted peers. |
| **Main** **Critique**: many legal cases say that regardless of privacy policy, can’t expect privacy! See SOLOVE 2008 for cases revealing lack of 4th amendment protection |
| **Citation: Ackerman, Mark, Trevor Darrell, and Daniel J. Weitzner. 2001. "Privacy in Context." Human–Computer Interaction 16(2-4):167-76.** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**:    What are the down stream consequences of providing data. How do we make this transparent? Do people care? Why not? How can we change this  User centered laws and regulations are infeasible and improbable to work consistently.  FTC guideline have no force of law and the government don’t comply either  Law enforcement can’t wiretap so commercial companies do and then resell to the government – that is nuts!  Popularity based trust systems (filter bubble) complacency issues. |
| **Bullet:** |

|  |
| --- |
| **Affiliative Trust-Mistrust 6-Point Coding Categories** |
| **Key** **Words**: |
| **Summary and Contribution**: ***6:***Relationships are depicted in very positive terms. In addition, there must be evidence of integration of problematic aspects of relationships, such as conflict and disappointment.  **5:** Relationships are depicted in primarily positive terms. There is trust, but it does not appear to have been tested.  ***4:*** Depictions of relationships contain material that can be coded for positive and negative categories, without a clear sense that the relationship is being strengthened through the resolution of problems.  **3:**Relationships do not work out because people are rejected, disappointed, or abandoned. Thus stories at this level often have a depressive, empty feel.  **2:** Depictions of relationships are centered around verbal hostility and cynicism. People are hostile, nasty, cruel, and dishonest toward others.  **1:** People are seen as threatening and extremely dangerous. This could include stories in which people fear for their lives, are beaten, sexually abused, or otherwise threatened with extreme maltreatment, and no one helps *them****.*** |
| **Main** **Critique**: |
| **Citation:** McKay 1991 |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: |
| **Bullet:** |

|  |
| --- |
| **The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors** |
| **Key** **Words**: Disclosure, Privacy, Intentions, beliefs, trust, risk |
| **Summary and Contribution**: It is often the case that societal expectations for privacy are in conflict with the prevalent, intimate, sharing, online.  Despite more conservative intentions and privacy complaints the authors examined and revealed actual behavior to be less rick averse and thus liberal with personal information.  Online behavior was different than offline with more risks taken online, with trust attained through fleeting mentions of security (privacy policies). The websites become the object of trust.  In the context of risk, an individual’s intentions and behaviours are not equal. |
| **Main** **Critique**: all student participants. Control for trust was attempted but educational setting might have skewed participant perceptions |
| **Citation:** Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." Journal of Consumer Affairs 41(1):100-26. |
| **Impact Factor**: 1.032 **Article Citations:** 157 |
| **Related to Identity Authentication**: obtaining trust in the absence of previous harm is relatively straightforward online, despite an individual’s awareness of risk |
| **Bullet:** Privacy policies for digital systems are only as secure as the behavior of these using the system |

|  |
| --- |
|  |
| **Key** **Words**: |
| **Summary and Contribution**: |
| **Main** **Critique**: |
| **Citation:** |
| **Impact Factor**:  **Article Citations:** |
| **Related to Identity Authentication**: |
| **Bullet:** |

## POSTER for DSTL

My research at Southampton explores new methods of identity verification and authentication that protect the individual by minimising disclosure to a level that meets service-provider needs whilst respecting user attitudes. In this sense, the aim is to develop an approach that puts the user at the centre of the agenda through understanding and designing issues of social acceptability and ethical practise

The research sits within the context of the [SuperIdentity project](http://www.southampton.ac.uk/superidentity/), which at its heart, is amassing identity-related information with the purpose of developing the means for highly robust identity decisions. Reverse-engineering this approach could give us the capacity to select appropriate value information rather than amass indiscriminately.

I am therefore attempting to enhance the development of verification techniques that rest on minimal disclosure by building my understanding of user sensitivities around disclosure, privacy and trust, whilst developing my technical skills in the analysis of digital mechanisms that readily compromise our privacy.

Technological progress in the area of digital identity provides fantastic capability but we may not yet have full awareness of its social acceptability or impact. The result is either that individuals readily over-disclose valuable information without awareness of the potential risks, or that they opt out of digital living through fear or lack of trust. Either way, the advances in identity technology may not yet serve the interests of all user groups.

The work described here will explore new methods of identity verification and authentication that protect the individual by minimising disclosure to a level that meets service-provider needs whilst respecting user attitudes. In this sense, we aim to develop an approach that puts the user at the centre of the agenda through understanding and designing issues of social acceptability and ethical practise

Methodology

The work outlined here sits within the context of the SuperIdentity project [2]. At its heart, this is amassing identity-related information with the purpose of developing the means for highly robust identity decisions. Reverse-engineering this approach gives the capacity to select appropriate value information rather than amass indiscriminately.

Two strands of work follow:

1. An understanding of user sensitivities around disclosure, privacy and trust;

2. The development of verification techniques that rest on minimal disclosure.

**Implications of work**

The value of this work is twofold. First, we will be able to respond to the risks recognised above by engendering trust through ethical minimal disclosure, thus protecting the user whilst minimising opt-out. Second, we will be able to respond to the continuing need from service providers to have robust means of authentication, whilst recognising the need for high value information only in high-risk contexts.

This approach to identity and authentication proceeds in synchrony with developments of legal understanding. In this sense, minimal disclosure offers a social and ethical response that protects both the user and the service provider.