# Progress and Reading List

This is a table of my first two term grades and weighting followed by a current list of relevant articles to my study.

|  |  |  |
| --- | --- | --- |
| **Term One** | **Final Grade** | **Earned** |
| Research Methods in Computing | 90 | 10.000 |
| Introduction to Complexity Science | 71 | 10.000 |
| Research Design & Multivariate Data | 79 | 10.000 |
| Advanced Computational Methods I | 79 | 10.000 |
| Foundations of Web Science | 61 | 20.000 |
|  | X = 73.5 | 60 Credits |
| **Term Two** | **Final Grade** | **Earned** |
| Complex Systems Simulation | 65 | 10.000 |
| Mathematical Modeling of CS | 63 | 10.000 |
| Further Web Science | 81 | 20.000 |
| Intelligent Agents | 83 | 20.000 |
|  | X = 76 | 60 Credits |
| Current Average = 74.75 | | |

### Module highlights and for future use:

Complex Systems Simulation – Modelling, complexity, system dynamics

Intelligent Agents – Game Theory, Strategy, Incentives

Research Design and Multivariate Data – Statistics, Visualisation, R

Further Web Science – Interdisciplinary Literature (Social, economic, political, Technical)

## Core Argument

Personal data is a commodity, which is traded between individuals and organisations at an ever-increasing rate. Facilitated by technological development and the ‘always on’ web, it is proving a difficult challenge to relate laws and regulations with capabilities and activities. Essentially a trade occurs when there is an interaction by a user with a particular ‘connected’ technology.

Currently there is a cost (time, money, attention) for users of technology to protect themselves from, or at least inform themselves of, any negative consequences. This cost coupled with an economic incentive for organisations to process and monetise data could lead to instability in user behaviours and potential be damaging to users who are perhaps naïve to the actualities and in addition, tempting to organisations pressured for profits. In essence this coupling can invoke periods of moral panic (users) and moral hazard (organisations) to the detriment of online activity.

However, by shaping the economic incentives on either side it may be possible to stabilise the environment and ensure a safe and engaging online future. Using the mechanisms of game theory to analysis the incentives and pay-off of this interaction, the feature of the online data exchange/interaction market will be simulated to reveal the suggested dynamics and possible influencing factors.

### Argument Logic

As user discrimination tends to zero the incentive for organisation to exploit increase.

As user discrimination tends to complete the incentive for organisation is to respect.

As organisation respect tends to complete the incentive for user discrimination decreases

(Villa et al. 2003)

If the cost of user discrimination can be subsidised then the dynamic becomes less volatile (reduce moral panic). Else if the cost of exploitation was increased this would reduce incentive (less moral hazard). Thus take from one side and give to the other.

# Titles of Readings

General Privacy Debates

1. Privacy in Context
2. Privacy in the clouds
3. Online privacy: a matter of policy?
4. Privacy and contextual integrity: Framework and applications
5. The Right to Privacy
6. Understanding privacy
7. Privacy as contextual integrity
8. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy

Technology – Challenges

1. Privacy and security of personal information
2. Forensic implications of identity management systems
3. I Know Where You are and What You are Sharing
4. Ambient intelligence: Technologies, applications, and opportunities
5. Privacy, identity and security in ambient intelligence: A scenario analysis
6. Biometrics and privacy
7. Privacy Weaknesses in Biometric Sketches
8. Making decisions about privacy: information disclosure in context-aware recommender systems

Behaviours

1. Privacy Paradox 2.0
2. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?
3. The privacy paradox: Personal information disclosure intentions versus behaviors
4. Young people, disclosure of personal information and online privacy: Control, choice and consequences
5. Social cognitive theory: An agentic perspective
6. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI
7. Reference points, anchors, norms, and mixed feelings
8. Regret Theory: An Alternative Theory of Rational Choice Under Uncertainty
9. Bounding rationality to the world
10. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields
11. What Firms Do? Coordination, Identity, and Learning
12. Collective Action and the Evolution of Social Norms
13. Evolution of collective action in adaptive social structures
14. Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias

Economics and Games

1. Markets and privacy
2. the market for" lemons": Quality uncertainty and the market mechanism
3. Nudging Privacy: The Behavioral Economics of Personal Information
4. When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information
5. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market
6. An Economic Theory of Privacy
7. The economics of privacy
8. Economic aspects of personal privacy
9. Game theory meets network security and privacy
10. A game theoretic framework for evaluation of the impacts of hackers diversity on security measures

Technological Solutions

1. Crime applications and social machines: crowdsourcing sensitive data
2. Privacy by design
3. Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment
4. Biometric encryption
5. Combining Crypto with Biometrics Effectively
6. An introduction to biometric recognition
7. Information accountability
8. Transparent accountable data mining: New strategies for privacy protection
9. Consent biometrics
10. Cancellable biometrics and annotations on BioHash
11. Adnostic: Privacy preserving targeted advertising
12. Biometric cryptosystems: Issues and challenges
13. Enhancing security and privacy in biometrics-based authentication systems
14. Using semantic web technologies for policy management on the web

￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼￼

## ￼ Development of a Social and Ethical Approach to Identity Assurance

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 practice.

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.

￼￼￼￼

# Brief Over View of Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task Type** | **Dissertation** | **Year One** | **Two** | **Three** |
| Literature | User Behaviours and Sensitivities on Identity and Privacy – the privacy paradox  Success factors of privacy technology  Legal and regulatory developments | Continue review. Explore the techniques used to limit information disclosure.  Understanding the value hierarchy of identity metrics. |  |  |
| Limits | Looking at individual interactions with commercial organisations | Broaden to include governmental activity |  |  |
| Exploration | Incentives and responsibility for privacy protection | Examine keystone identity metrics on which high social and regulatory value can be places |  |  |
| Aim | To examine the incentives for privacy preservation between users, designer and regulators | To justifiably indicate which identity metrics are appropriate for a given level of authentication requirement. |  |  |
| Theory | Sufficient privacy awareness is needed to shape privacy provision.  Even with improved privacy awareness through education and nudge, a disjointed approach to privacy by design is not sustainable. A platform or interface would be required to provide consistency and allow creativity (see Recordon and Reed, 2006). Furthermore the entire system is likely to rely on accountability and enforceable regulation.  By understanding the mechanisms used to piece together identities across real and cyber domains it may be possible to help focus effort on the restriction of keystone identity metrics so that diverse attempt to incorporate privacy by design may have a shared principal. | | | |

The Eighth International Conference on Digital Society

ICDS 2014

<http://www.iaria.org/conferences2014/CfPICDS14.html>

March 23 - 27, 2014 - Barcelona, Spain