A game theoretical examination of user and service privacy incentives

a case for privacy ??? engineering and education

“The panic about privacy has all the finger pointing and paranoia of a good old scare, but it’s missing one vital ingredient: a genuinely alarmed public. [People] care about privacy mainly in the abstract.[2008????]”

# Abstract

Some words here ;)

### 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

## Introduction

Right or wrong, there is a market for personal information. Personal information is amassed, processed, mined, repurposed, extrapolated upon, stored, traded and stolen on a global stage. Personal data has always been a commodity, so it is no surprise that people and organisations have found a way to monetise it and or exploit its value. The Internet is simply the catalyst making this process efficient and attractively profitable. The scale and the increasing sophistication of operations have heightened concerns (which have long existed) to a global level. Yet the profits and benefits of data utilisation are easier to define and defend than any current articulation of the concerns about such practices. Thus ‘privacy’ is held up often intrepidly to place scrutiny on certain practices and illuminate the concerns of many antagonists. Unfortunately the multifaceted use of the term privacy has further muddled its meaning and is perhaps diluting any desired effect (Arther Miller in Solove), leading to some academics either tentatively deploying the term or creating new terms to define the old concept. Simply put the effectiveness of the word privacy is perhaps facing the same fate as the concept it is defining. () suggest pro-privacy commentators avoid the term altogether, Nissenbaum uses ‘contextual integrity’ to propose an alternative legal framework for what is essential the protection of privacy. Whilst Solove (2007) remarks that privacy has so long been held up as the adversary of national security that ‘it is hard for privacy to prevail’.

Another pragmatic yet slightly conceding perspective was to stop resisting and join the data utilisation process, albeit with the gains being realised by the individual owners of the data “Why not let individuals own the information about themselves and decide how the information is used?” (Laudon, 1996). This question, posed almost two decades ago, depicts a society were profits can be harnessed by individuals for information about themselves. This economic view stems from a concession that privacy is in decline and this trend is likely to continue, therefore we can strive to make the best of the situation. In essence, a thought could form such as, if my data is making a profit for someone else, then I should see my share. The reality however is closer to this than we may think. Individuals do ‘sell’ their information on a daily basis. Individuals can and do ‘profit’ from this trade, just not in a financial sense or in a consistent manner. Individuals are trading their information for the free use of media software, the chance to win a prize or the ease of e-commerce.

So what is the problem? Or at least what problem does this paper look to address? The answer to this question is twofold. Firstly, technology advancements have increased data processing capabilities, which continue to develop and outpace the scope or reform rate of the laws and regulations. Resulting in a ‘legal void’ (levesson) within which only a hazy and inconsistent understanding of what is right and wrong persist, thus leaving decisions to the ethics of the corporate world. Secondly, regardless of this opaque world of data utilisation, individuals are subject to an ever-present, asymmetrical negotiation where our trade-off considerations are often masked by naivety (“nothing to hide”, “small price to pay for national security”, Solove, 2007), a sense of vulnerability (nothing I can do to stop it) or even apathy (“No bodies on the street”, Villa, 2003). Therefore the trade-off is quite far from the conceived market equilibrium price in a ‘National Information Market’ that Laudon proposed as an economic solution (ibid)

This collection of claims and observations (amidst others) by academic and legal commentators will be unpacked in section two, however, before this is possible it is important to define the often muddled terms which will run centre to my dissertation.

So instead of throwing privacy out, an attep to strenten it could be more fruitful.

Contextual Privacy

Ethical Privacy

Corporate Privacy

Domestic Privacy

Social Privacy

…

Instead a game theory approach is used to help understand and explore user behaviours and service provider practices regarding personal information, by considering the incentives for service users to give and service providers to accumulate data. Furthermore, this approach can help highlight the boundaries at which these behaviours may change.

## Structure

To achieve this task the paper will commence with a literature review on five principle pieces. First a review on privacy related user behaviours such as the privacy paradox, where the current extent of personal information disclosure and the acknowledged risk of doing so are unaligned (Norberg et al, 2007).

Then a review on the economic value of personal information to organisations and how this value allows for the provision of sophisticated systems for free ( ) and how this value encourages the assembly of further information and moreover the inference of unknown information (turning lead into gold)

Third the risks

Forthly the review will focus on the legal frameworks enabling significantly sized personal data exchanges. Notably how the advent of the Internet has provided a new context for old laws. Hence the call for updated laws and claims of legal operations (Legal void) contextual integrity.

The final piece looks at various methods proposed to control if not limit the uninhibited utilisation of personal information, from user education and awareness to, privacy by design.

These pieces will form the basis of the game analysis to understand that if the enduring message from many privacy discussions is that privacy is something to preserve and respect yet legal, ethic and technical systems are lagging behind the curve relative to those able to exploit personal information. The questions remain, what to do, how to do it and by whom?

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

Overview of intentions and model approach

### Current Affairs/context

Despite privacy being a longstanding, key social issue, arousing much academic, political and legal deliberation, the subject has rarely received such a sustained public deliberation as in the case of Edward Snowden [ ]. The ingredients of this story may just provide the catalyst for change which many pro-privacy commentators call for. An American CIA technician seeking asylum across the globe after revelling information about US surveillance operations involving the social communication tools millions of people use daily [ ]. If the missing ingredient of a real privacy panic was a “genuinely alarmed public” then this may have provided it. Alternatively the status quo may resume and the Snowden case may prove to be a considerable yet controllable PR failure in a genuine pursuit of global security.

Whilst the details and potential consequences of these events unfold this paper looks back and examines the environmental and behavioural developments in the backdrop of the Snowden saga and why these revelations are concerning yet not fully surprising. please note that any judgement on either the Snowden case or the general issue of privacy versus liberty will be reserved for other forums.

## Defining Privacy

## Understanding Privacy

What is Identity, which part of the privact parcel am I looking at.

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 |

## Users

Despite a reported concern regarding the risk of online transactions or interactions especially around fraud, identity theft and privacy, a typical users’ actual behaviour is far from risk averse ( ). There is a tendency to consider the dangers of online interactions in the abstract whilst in practice exhibit carefree behaviours. Many commenters believe this paradoxical behaviour is thwarting attempts to regulate and encourage ethical organisational behaviour or increase user mindfulness towards their self-protection.

It has been suggested that users are acting as rational agents when interacting with online systems and are capable of understanding the trade off between what they are providing (cost) and what they are obtaining (gain). Others suggest that it is either impossible or impractical (given resource limits) to comprehend the intricate trade-off due to the asymmetrical information held by each entity (economics of privacy).

Regardless of the clarity of trade-off, users appear quick to provide, potentially high value, data for seemingly low value returns and for those unwilling to make this trade the alternative is often to restrict online use or abandon it. If users are acting rationally then this (current trade off) is the likely stable state of the system and those restricting their access, if in the minority, will continue to be marginalised. However if user, by some mechanism, became more discriminate about the value of their own side of the trade, then a rebalance of the system is plausible and those opt-out users may be introduced to inflate the market value (lemons ??).

This trade off dynamic will be the core of this paper’s argument and the model in a later section.

### Digital living opt out

The decision to opt out of online interaction alone is not much value in the pursuit of protecting oneself. It may be a fallacy to consider the risk of the cyber world to be distinctly delimited from the real world since the connectedness of digital devices range from satellite navigation, mobile phones, retail accounts, travel, banking etc. the risk of id fraud is constant since we allow so much of its composition factors to remain public. Offline interactions form part of the bigger picture so by limiting online interaction a person is simply limiting the picture but not eliminating it. Increasingly both cyber and real world data is combined, processed, extrapolated upon and repurposed to create a commodity, which is sold for profit. This is big business fuelled by all types of digital living, thus resistance is difficult, avoidance could be infeasible, thus the trade off of using the internet or not is heavily bias towards using since the risk are always present.

### Privacy paradox

Nonetheless there seems to be a behavioural paradox between

What governs users behaviour online?

Free services v personal information valuations

Instant gratification v intermittent concerns

Bounded rationalisation V Complex decsions

What incentives do services get from privacy?

### Identity

SID, identification dn authentication

### Legal development/ issues

Contextual integrity

## Value of Identity data.

The trade offs. Value of service, instant gratifcaition,

Here I use a simplified trade-off matrix to examine ‘player’ strategies under changing conditions. To help understand the influences and key parameters o fhte interplay to help focus any future interventions. The model shows that user mindfulness’ is a key component of the interplay but as the argument progresses the influence of user behaviour alone is not a stable outcome and thus is necasary but not sufficient to creat sustained (respectful) system behavour

Respectful and mindfulness: define this concepts.

The context of this thougt experiment: when the cost of privacy (Respect) is borne by the organisation only the user can discriminate between organisations without without respectful intentions, yet the number of users willing or able to discriminate between organisations makes a difference to the statigies chosen by organisaitons in pursuit of profits. Without discrimination the cost of privacy doesn’t add value to the organisation and prevents a particular revenue stream. It a double edged sword which wil be hard for stakeholders to swallow. However as mindfulness increases, it seems that smaller cmapnies in the first instance can benefit from privacy investment and begine to consume larger market share making the investment worthwhile, until a point where larger organisations are strategically incined to follow, thus respoting market balance (albeit at lower margins). There are a number of asumtion here, namely the pure finantial driven startegies of the organaistions whereas other emotive factors may influence strategic decisions. Especially when margins are tight and a clear trend is emerging.

Behavioural economics of privacy

25 cents

### Misunderstandings

Lemons market

Bodies on the Street

At this point I wish to go back to the start, I wish to question the need for such vigilance in the first instance. The difficulties involved in even defining privacy and he inconsistencies of privacy expectation along with the practical problem of implementation and investment. Instability in the system dynamic may suggest it just isn’t worth it (financially). given privacy arguments are often juxtaposed with security ones in a potentially misleading or at least misunderstood way, it maybe that unchecked or scrutinised and the choice will may be between scrutiny and liberty and not a case of the appropriate and possible perennial rebalancing of the two.

In the argument – nothing to hide/ counter terrorism -> small price to pay (fear), practical obscurity/ what is harm – no bodies on the street.

Trade-Off

User: instant gratification, popularity based trust, novelty, uncertainty (poem if a friend is not a friend or foe…” ) policy based / seal trust. No economic cost.

Difficult to read policies, will happen anyway, nothing to hide. No connection between event and harm (inconvenience hard to source) data is already out there. Where is origin of leak? My phone call? Where is the transparency. Cheap attention grabbing lie.

Trade of Organisation:

Hold up under scrutiny, social Corporate responsibility, ethical workplace/ reputation

Far from the money, the harm easy to just defeat emotionally, everyone is doing it. Can rationalise the action and therefore incentive to deceive. Shareholder pressure again far from the money/harm. Data can still be breached anyway, the data is public so why don’t we profit from it

### 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

“It is easier to imagine the end of the world than the end of capitalism” (future city, 2003 Zizek and Fredric Jameson

## Risks and Harm

What are the risks are they real, are they being realised. Who care and who is doing it. Is it purely for profit, is it a bad thing, can we benefit from it, tangible and intangible.

### National Security

Intrusive power

Zero sum game!

## Privacy Protection

Two perspectives have formed to address this issue, each either side of the user-technology interface. On one side there are advocacies for promoting user privacy education, wherein users take an informed responsibility for the protection of personal information (Orgill et al, 2004). Whilst the others focus on privacy by design, ensuring services follow sufficient privacy protocols and regulation on the design side of the interface (Cavoukian, 2009).

Previous research into the privacy paradox has looked at the decision process and the associated cost-benefit to an individual’s privacy trade-off (Acquisti. 2009). This economic perspective lends well to similar game theory analysis, therefore I aim to conduct a game theoretic study to explore the impact and interplay between the above perspectives and how this may affect a user and or service privacy trade-offs.

By simulating various scenarios based around users’ privacy education and the cost benefit for organisations to enhance their privacy by design measures. The proposal is that low privacy education in the context of the privacy paradox, provides little incentive for services to invest in privacy engineering, yet under certain conditions the cost benefit threshold is crossed in favour of privacy.

### Digital solutions,

### Legal protection and self regulation

Context aware computing

### Transparent data mining

Education

TAMI – wish to represent laws in N3

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

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

## A simple game

First model of privacy strategy and economic incentive. A 2 player game theory approach. Two orgs competing for a N population customer base. Zero sum game.

Game theory accounts of privacy and security, gloabal cyber game

## Concept

Two companies Cvast.com and Clight.com provide similar services and have a healthy number of continuing users and a steady flow of new users. Both services are free, however a user must provide identifying information, which is used for targeted advertisements to generate revenue. The companies form a zero sum game, wherein a user is considered to join only one service, although they can switch allegiances.

### Simplified Operating Costs

Revenue per user = £1.00

Cost of Service per User = £0.20

Cost of Privacy Measures = £0.10

Privacy Reduced Revenue = £0.20

It is easy to calculate from these numbers that privacy measure will vastly reduce revenue per user, leading to a dilemma. If Cvast.com does not use privacy measures and therefore maximise their profits per user, what strategy is best for Clight.com?

BP = Base Profit per User = £1 - £0.20 = £0.80

PP = Privacy Profit per User = £1 - £0.20 - £0.10 - £0.20 = £0.50

### Simplified User Preferences

A user is happy to use either service but will have a bias based on popularity. In addition a user has a level of privacy mindfulness that can determine which service to use.

Cvast.com is currently more popular than Clight.com

### Service choice.

Popularity of Cvast.com (PoPvast) + Clight.com (PoPlight) = 1.0

Mindful Users + Naïve Users = N

Revenue £ = Popularity \* N \* Profit per user

### Case 1: No Privacy Mindfulness

If N = 1000 and PoPvast = 0.5 and Mindfulness = 0

HP = 0.5 \* 1000 \* 0.5 = £250

LP = 0.5 \* 1000 \* 0.8 = £640

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Cvast.com | | With no privacy mindfulness, there is no incentive to provide privacy features. NE is no privacy measures |
|  |  | Privacy | No Privacy |
| Clight.com | Privacy | £250, £250 | £250, £640 |
| No Privacy | £640, £250 | £640, £640 |

### Case 2: Popularity difference

If N = 1000 and PoPvast = 0.75 and Mindfulness = 0

Cvast: HP = 0.75 \* 1000 \* 0.50 = £375 && LP = 0.50 \* 1000 \* 0.80 = £600

Clight: HP = 0.25 \* 1000 \* 0.50 = £125 && LP = 0.25 \* 1000 \* 0.80 = £200

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Cvast.com | | Even with popularity differences the NE remains no privacy measures |
|  |  | Privacy | No Privacy |
| Clight.com | Privacy | £125, £375 | £125, £600 |
| No Privacy | £200, £375 | £200, £600 |

## Mindfulness

So far the cases have been trivial, with a cost incurred for no financial benefit to either company. The only benefit would be organisational value and ethics. In this case the mindfulness vaiable is changed to provide an incentive for privacy measures.

Now ½ the population will discriminate based on privacy provision. Thus both companies share out the naive population based on popularity and either share the mindful population with the same ratio if both adopt the same strategy else the sole privacy conscious company gets all the mindful users.

Cvast Strategy Revenue

If Clight Strategy = HP

HPExtra = POPvast \* MP \* PP

LPExtra = 0

else

HPExtra = MP\* PP

LPExtra = PoPvast \* MP \* NP

vastHP = PoPvast \* NP \* PP + HPExtra

vastLP = PoPvast + NP \* BP + LPExtra

Clight Strategy Revenue

If Cvast Strategy = HP

HPExtra = POPlight \* MP \* PP

LPExtra = 0

else

HPExtra = MP\* PP

LPExtra = PoPlight \* MP \* NP

lightHP = PoPlight \* NP \* PP + HPExtra

lightLP = PoPlight + NP \* BP + LPExtra

### Case 3: Mindfulness

If N = 1000 and PoPvast = 0.75 and Mindfulness = 0.5

LP = 0.50 \* 1000 \* 0.80 = £600

Clight: HP = 0.25 \* 1000 \* 0.50 = £125 && LP = 0.25 \* 1000 \* 0.80 = £200

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Cvast.com | | Even with popularity differences the NE remains no privacy measures |
|  |  | Privacy | No Privacy |
| Clight.com | Privacy |  |  |
| No Privacy |  |  |

I Privacy mindfulness = 0 for all population (N) then service discrimination dependent on service popularity.

## A second complex model

Over time, the dynamics approach and return from unstable equilibrium points, the actual systems (utopian) involves risk and harms and adequate protection. Using agent based social cognitive theory model to illustrate the log term challenges with privacy respect online

The dynamic gets slightly more problematic when all organisations become respectful since users can afford to be less discriminate, less vigilant and less concerned. This reintroduced an incentive for an organisation to defect from the respectful position in pursuit of greater gains from unsuspecting users. Such opportunities behaviour makes the whole system unstable (). If revealed this could damage an organisations reputation, but who is looking? Examples of previously bad press, short-term pain. Not enough bodies on the streets for lasting public awareness and subsequent intervention

Villa et al, consider a central independent body (government) as a prime entity to continuously test and monitor organisations behaviour, yet the same incentive applies, analogues to police on the streets, f no crime is being committed the incentive is to cut policing costs yet this increases dark spots where opportunistic crime may occur. Online such constant vigilance could be conducted through auto systems/ browser warnings, seal based systems. P3P but these systems are bounded in theory application and usefulness and fail to account for contextual transgression.

Transparent data – phone call – where did you get my number? From A via B….

The model here depicts a dichotomy of respectful and defecting organisations which vastly over simplifies the situation, nissenbaum writes of contextual integrity and in practice this account of privacy related transgression is intuitive and progressive yet is difficult to generalise into strict logic for a computer to interoperate or even for an organisation/ policy maker or user to interpret and define in a particular context. Plus the burden is still on the user to understand the transgression and their rights. Cases of self-regulation being purely lip service. What is the point? How can integrity be installed in a systems and thus how can lack on integrity be penalised how is judge and jury?

## 

## 