The Identity Trade: A Game Theoretical Approach

“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 .[200?]”

# Introduction

The ability or need to manage our identity in the digital age has underpinned much academic and political debate. The extent and reach of the debates surrounding identity, not least privacy disputes, increased identity theft and reported large-scale espionage, denote identity as a key social issue which will continue to vigorously engage and challenge the policy makers, the judicial reformers, social campaigners and technology designers on a global level. At the heart of many a deliberation is whether advances in identity technology serve the interest of all user groups and therefore whether they are legally or social acceptable. The argument is convoluted further and perhaps heightened by the direct conflict between recent advances in technological capability for national security interests and longstanding individual privacy values. Technological capabilities, which can be operationalized by non-security organisations to arguably the detriment or benefit of society under the shade of a legal void. Furthermore a legal void in terms of what is permitted from organisations processing identity data creates an environment where opportunistic, quasi-ethical behaviour could threaten social norms and values.

Any uncertainty could be associated with undesirable outcomes such as the willing and regular over-disclosure of valuable information, by individuals seemingly unaware of the potential risks, or with a level of awareness resulting in fear and lack of trust towards an ultimate opt-out from digital living.

There have been a multitude of approaches to develop privacy-preserving technologies or to define laws and regulations to encapsulate the appropriate balance between the value of identity data and the social concerns. This paper looks at some of these legal, technological and regulatory developments and aims to highlight what the imbalance may be and therefore pursue a roadmap to inform the future developments of technical and governmental initiates.

The work here follows two strands, the first is an understanding of user sensitivities around disclosure, privacy and trust, whilst the second is an examination of the incentives which may be frustrating attempts to realize a stable interplay which promotes legal, ethical and social acceptable behaviors by individuals and upon individuals.

## 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). Followed by a review on the economic value of personal information to organisations and how this value allows the provision of sophisticated systems for free.

Thirdly the review considers the risks and consequences of users willing and regular trade of personal information for the convenience and access to digital services of vastly varied quality and benefit. Fourthly the review will focus on the legal frameworks enabling significantly sized personal data exchanges and how the advent of the Internet has provided a new context for old laws.

The final perspective concerns the various methods currenlty proposed to control if not limit the uninhibited utilisation of personal information, from solutions that encourage user education and awareness or technological systems incorporating privacy by design.

These pieces will form the basis of a game theory 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?

## User Behaviours and Attitudes

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 ??).

### 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 decisions

What incentives do services get from privacy?

### Identity

SID, identification dn authentication

### Legal development/ issues

Contextual integrity

## Your Information Market

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 and people and organisations have found novel ways to exploit its value over the ages and more recently monetise it (Laudon, 1996). The growth of the Internet and accompanying data processing technologies has simply been the catalyst increasing the efficiency, profitability and direct trading of personal data. However it is arguably this new scale and the increasing sophistication of data sharing operations, which has heightened concerns (which have long existed) to a global level. The added explicitly and occasionally newsworthy revelations of personal data exchanges, is adding to the public concern.

Nevertheless, 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. Barkhaus (2012) suggests that 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’. Given privacy defence arguments are often juxtaposed with security ones in a potentially misleading or at least misunderstood way, it could be that, unchecked or lack of credible scrutiny, the choice may be security or privacy and not the appropriate and possible perennial rebalancing of both (Bin in Jain et al., 2004)

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 of my information market. The reality however is closer to this than we may think. Individuals do ‘sell’ their information on a daily basis. Individuals can and do ‘receive’ 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 whilst there is a receipt in this trade just as in any commodity trade it is unclear as to the division of profits since the negotiation is heavily skewed due to individuals acting on incomplete information and thus a possibly low valuation of what they are giving.

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 (“resigned”, aquisti 2010) 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)

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. An environment where the symmetry of information has a balance of informed traders on both sides. 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.

### Market Instability

Villa et al, (2003) extends a ‘lemons market’ concept offered by Akerlof (1970) to describe the current situation with online data trades, signifying the asymmetrical information and uncertainty as a key reason for instability between seemingly risky behaviour and potentially deviant incentives. These authors argue that the situation is cyclical such as

1. As user discrimination tends to zero the incentive for organisation to exploit increase.
2. As user discrimination tends to complete the incentive for organisation is to respect.
3. As organisation respect tends to complete the incentive for user discrimination decreases
4. Repeat

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

### Protection of ‘privacy’

To protect privacy, it may be prudent to begin with the protection of the term itself. The continuous re-defining of privacy and attempts to supersede the term altogether can only cause delay whereas the counter pressures of the terms ‘security’ and ‘profits’ need little interpretation and therefore proceed towards domination whilst ‘privacy’ sufferers existential uncertainty.

### Responsibility?

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).

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

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.

## The informed trade

### 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.

## Understanding Privacy

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 |

## Value of Identity data.

Here I use a simplified trade-off matrix to examine ‘player’ strategies under changing conditions. To help understand the influences and key parameters of the 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 necessary but not sufficient to create sustained (respectful) system behaviour

Respectful and mindfulness: define this concepts.

The context of this thought experiment: when the cost of privacy (Respect) is borne by the organisation only the user can discriminate between organisations without respectful intentions, yet the number of users willing or able to discriminate between organisations makes a difference to the strategies chosen by organisations 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 will be hard for stakeholders to swallow. However as mindfulness increases, it seems that smaller companies in the first instance can benefit from privacy investment and begin to consume larger market share making the investment worthwhile, until a point where larger organisations are strategically inclined to follow, thus restoring market balance (albeit at lower margins). There are a number of assumptions here, namely the pure financial driven strategies of the organisations whereas other emotive factors may influence strategic decisions. Especially when margins are tight and a clear trend is emerging.

## 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.

### 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

# A Privacy Strategy Game

I wish to pause to take consideration of a simple strategy game between two competing companies Cvast and Clight. Both provide similar services for free, however interaction with the system involves a user continuously providing identifying information. This information can be processed and has a market value according to quantity. Each organisation can choose to exploit the data for extra revenue per user. The decision to exploit or not depends on a 2 player strategy game detailed below.

The main revenue model for each organisation is based on advertisement. Advertisers will pay depending on the size of user base. Furthermore they will pay more if they are given the personal information and thus be able to better target their adverts.

The companies form a zero sum game such that a user will join just one service, although switching is possible. Users fall into two categories, Aware or naive. An aware person person will join a respectful company if given a choice and a naïve person will not discriminate between respectful and defecting companies. If there is no choice since both companies adopt the same data strategy, then a person, aware or not will join a service at ratio proportionate to the company’s popularity.

Revenue Calculations: these are produced on a curve to sugest a non linear relationship between usrs and advertisement appeal.

Population size is set at 100000

Awareness of the population is a 0 – 100% ratio of the population

Popularity of CLIGHT + CVAST = 1

### Main assumptions and simplifications

No operating costs.

No cost to switch organisation

Organisation popularity is pre set.

Transparent strategies for organisation

Binary state for population (aware or not)

Rational profit maximising organisations

## Two Bounding Cases:

|  |  |
| --- | --- |
| **PARAMETERS** | |
| POPULATION | 100000 |
| AWARENESS | Variable |
| NAIVENESS | 100% |
| POPULARITY\_CVAST | 95% |
| POPULARITY\_CLIGHT | 5% |

For a moment lets consider two cases, one where the population is unaware and a second when the population is fully aware. These extremes are rather unrealistic yet serve to set the boundaries for further cases of partial population awareness.

### Case one: ZERO Awareness

In this case there in no incentive for either organisation to respect personal data despite what the other organisation does, so exploitation is a dominant strategy, a Nash Equilibrium and Paraeto Efficient. The case is trivial since no mater what strategy is played the population are not aware and therefore are not discriminate about he organisation they chose, so each organisation will incur a cost (reduced revenue) but no financial gain.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | CVAST | |  | OUTCOME | CVAST | CLIGHT |
|  |  | Respect | Exploit | Dominant Strategies | Exploit | Exploit |
| CLIGHT | Respect | £1827, £77508 | £1827, £164174 | Chosen Strategies: | Exploit | Exploit |
| Exploit | £3015, £77508 | £3015, £164174 | Nash Equilibrium: | Exploit | Exploit |
|  |  |  |  |  |  |  |  |

### Case Two: COMPLETE Awareness

Not surprisingly, the scenario where the population is completely aware and discriminate over which organisation to use yields a different outcome. In this case the Nash Equilibrium is to Respect yet the Pareato Efficient outcome is to exploit. If both organisations colluded to exploit the data both would be better off than the reduced revenue ‘respect’ strategy. However the game principles concur that the incentive for CLIGHT in this case is to defect from this strategy to gain the higher (in this case all) market share and therefore profit.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | CVAST | |  | OUTCOME | CVAST | CLIGHT |
|  |  | Respect | Exploit | Dominant Strategies | Respect | Respect |
| CLIGHT | Respect | £1827, £77508 | £78146,  £0 | Chosen Strategies: | Respect | Respect |
| Exploit | £0, £78146 | £2347 £112804 | Nash Equilibrium: | Respect | Respect |

These basic scenarios suggest that at some point, increased user awareness has caused a tipping point in the dominant strategies of these companies. With a little further investigation we can see where and what (under these conditions) that tipping point entails.

## The Tipping Point

Figure (xxx) starts to revel the interplay between awareness and organisation strategy. The three parts relate to revenues, chosen strategies and dominant strategies. Qualitatively the situation changes from a Nash Equilibrium of exploiting data to CLIGHT finding a niche profit via respectful strategy. This can explain the various services such a ( DuckDuckGo ) and (…) which are tryng to forge sucees from adopting a respectful stategy and attracting users who are aware and discriminate in their online interaction.

Under these parameters it then take a long push in the awareness of the population before CVAST has the incentive to deviate from exploiting strategy and follow the respectful operations of the competitors. This looks disastrous for CLIGHT as CVAST regains the market share, albeit at lower profits. However as we add a few more dynamics to the model we can see that this need not be the case.

A closer look at the dominant strategies in figure () show that both organisations enter a period of strategic uncertainty, CLIGHT, followed by CVAST and it is this period where the switch to respectful strategies can occur. The argument follows that in an environment with enough discriminate individuals (high awareness) the safe strategy is to cater services to this section of the population whilst automatically providing a service to the rest of the populations should they choose. i.e, smaller companies can least afford to reduce their user target group compared to larger organisations who can absorb the absence of smaller user groups.



## Model Extensions

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.

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?