Macroeconomics of privacy and security for identity management and surveillance

Katos, Vasilios; Stowell, Frank; Bednar, Peter

Published in:
Kybernetes

DOI:
10.1108/03684921311295538

2013

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Macroeconomics of privacy and security for identity management and surveillance

Vasilios Katos
Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece

Frank Stowell
Department of Computing, University of Portsmouth, Portsmouth, UK, and

Peter Bednar
Department of Informatics, University of Lund, Lund, Sweden

Abstract
Purpose – The purpose of this paper is to develop an approach for investigating the impact of surveillance technologies used to facilitate security and its effect upon privacy.

Design/methodology/approach – The authors develop a methodology by drawing on an isomorphy of concepts from the discipline of Macroeconomics. This proposal is achieved by considering security and privacy as economic goods, where surveillance is seen as security technologies serving identity (ID) management and privacy is considered as being supported by ID assurance solutions.

Findings – Reflecting upon Ashby’s Law of Requisite Variety, the authors conclude that surveillance policies will not meet espoused ends and investigate an alternative strategy for policy making.

Practical implications – The result of this exercise suggests that the proposed methodology could be a valuable tool for decision making at a strategic and aggregate level.

Originality/value – The paper extends the current literature on economics of privacy by incorporating methods from macroeconomics.

Keywords Macroeconomics, Surveillance, Security, Privacy, Ashby’s law of requisite variety, Information systems, Decision making

Paper type Research paper

1. Introduction
In this paper we raise questions about the effectiveness of what appear to be policies regarding the installation of surveillance technologies. We ask if such technologies are eroding individual privacy. In this paper we investigate whether it is possible to strike a balance between surveillance as a means of citizen protection and at the same time preserve privacy, since “new technologies mean that the consumer can unwittingly become the integral part of a data collection system” (Rudall and Mann, 2008). In the context of the paper the term “surveillance technologies” is used to describe all monitoring technologies that continuously capture data on a wide scale.

A preliminary version of this paper appeared in Data Privacy Management (DPM) 2010.
1.1 Variety, control and heuristics
If we assume that the purpose of surveillance is to exercise control over a situation it monitors, e.g. crime reduction, terrorist activities, then we must take into consideration both the subject and the means of monitoring that subject. To this end we reflect upon Ashby’s argument that in any situation:

[...] if a certain quality of disturbance is prevented by a regulator from reaching some essential variables then that regulator must be capable of exerting at least that quantity of selection (Ashby, 1960, p. 229).

In other words the variety in the controller must have as much variety as that which it seeks to control. This revelation became known as Ashby’s Law of Requisite Variety (LRV) which explains that in order to bring about effective control over any situation the control mechanism must be capable of addressing as many different outcomes that it is possible for a situation to develop. The more complex the system the more difficult it is to predict its behaviour and the more difficult to exercise control. As a reminder of the practical difficulty Sir David Pepper the recently retired Director of GCHQ (the UK’s surveillance centre) said, “You would have to have so many people involved in the security services I am not sure what anybody else in the country would do” (Pepper, 2009).

It is axiomatic that in order to manage complexity we need to reduce its variety and by thinking in terms of, “[...] heuristics rather than algorithms which, as Beer reminds us that it is”, “[...] at once a way of coping with proliferating variety [...] instead of trying to organise it in full detail, you organise it only somewhat; you then ride the dynamics of the system” (Beer, 1981, p. 53). The present surveillance policy seems to be one of collect as much information as possible in the hope that some of it may be useful at some time. This policy is exemplified by the unofficial eavesdropping by the National Security Agency (NSA), who are said to save all communication data for future use (Harris, 2006) an approach underlined by a comment by a security expert who declared that “If you can’t find the needle, you have to take the haystack” (Harris, 2006). A control system seeking to control every conceivable eventuality generates so much variety that it is impossible to analyse and control it. The only strategy open to us is to reduce variety and simplify the situation into one over which we can exercise some degree of control.

1.2 Surveillance and privacy
In 1968, concerns were raised about the level of the US Government surveillance activities. Christie (1968) pointed out that the growing level of surveillance was having an impact upon the exercise of freedom of speech despite the claim that it had become necessary on the grounds of protecting its citizens. Concerns were also raised by Christie (1968, p. 876) about the threat to individual self-respect since, “[T]he individual can never be sure that he is not under government surveillance whenever he walks the streets”. The consumer privacy surveys by Westin (1991, 1994, 1996, 1998) which are run on a regular basis have consistently revealed a high level of public concern about privacy. K. Taipale, Executive Director of the Center for Advanced Studies in Science and Technology Policy proposed that FISA should be modified to allow for the electronic surveillance equivalent of a Terry stop – under US law which says that in order to apprehend a person the police officer has to have a legally based reason of suspicion. If we consider this in the context of automated data mining it has been pointed out that if the officer’s suspicion was subsequently unjustified the monitoring should be discontinued (Harris, 2006).
In 2003 Congress terminated the Total Information Awareness (TIA) project because of widespread criticism that as it had been acquired by the NSA it would create Orwellian mass surveillance. Surprisingly the classified annex written by the legislators preserved the TIA’s component technologies funding when transferred to other agencies (Williams, 2006). Despite the immensity of the task of monitoring and control in 2001 the UK Government in 2001 announced £79 million state spending on more CCTV systems. The impact of this programme has produced some startling results. For example, in one 650-yard section of Holloway Road in London there are 29 cameras: a crime-ridden high street in north London has been branded the most spied-upon road in Britain after it emerged that it is watched over by more than 100 closed circuit television cameras (Beckford, 2007). A survey by the US General Accounting Office in 2004 reported that federal agencies were involved in 199 data mining projects of which 122 used personal information (US General Accounting Office, 2004). Amongst other reasons these projects aimed to be used in the investigation of criminal and terrorist activities.

1.3 The challenge
The question we raise is what impact are the measures ostensibly being set up to strengthen security having upon each citizen’s right to privacy? To this end this paper is an account of an attempt to develop a decision support tool to assist in strategic and aggregate decision making relating to surveillance. The LRV suggests to us that such policies cannot achieve the desired end of full protection and we argue that continuance of such policies will erode individual privacy. As a consequence we reflect upon alternative strategies and describe a methodology that we believe to be useful to decision makers. The paper includes outcomes from empirical studies in which attitudes and concerns about the use of personal data were revealed which provide support for the contention that there is a growing unease about the use of technological surveillance.

2. Privacy, surveillance and transparency
There is no universal definition of privacy but it is reasonable to argue that its loss, whenever it happens, is recognised. It is an expectation shared by citizens in a civilised and democratic society (Privacy International, 2007). This is not a new concern as in 1995 a report by the US Department of Commerce (1995) commented that surveillance combined with the power of technological manipulation has the potential of eroding individual liberties irrespective of the apparent justification. Since that time increasing surveillance is viewed by many as an erosion of privacy despite claims that it is a means of improving the security of the population (Wright and Kakalik, 1997; Koops and Leenes, 2005; Dalal, 2006). Richard Thomas, the Information Commissioner and the UK’s privacy watchdog, has stated that we are sleepwalking into a surveillance society (Streeter, 2007). He has grown increasingly alarmed by the erosion of privacy and the extension of state surveillance; Thomas is quoted as saying that public confidence in surveillance technology needs to be restored (Johnston, 2007a, b).

Common sense suggests that laws passed prior to the developments in communication technologies and the web are now likely to be deficient. There should be a clear relationship between actions taken to protect citizens and their right to privacy. In most Western cultures privacy is protected by legislative means and the security controls presently introduced may raise legal and ethical conflicts (see for example the Proportionality Principle included in the EU Directive 95/46/EC). Our view is that
it is desirable to understand the relationship between security and privacy in order to
detect or predict – at the very least – policy violations caused by security controls.
We offer a model showing the relationship between the two that will contribute to
providing reassurance to the population who may feel uneasy about the present policies
on surveillance.

3. Surveillance and modelling
Modelling the relationship between surveillance, security and privacy means that
certain assumptions have to be made as any model of such a situation is a simplification.
Because of the unlimited variety in the system it is impossible to give a full specification
and impossible to produce an exact algorithm. As Beer (1981, p. 53) points out “The
strange thing is we tend to live our lives by heuristics and try to control them by
algorithms.” But in adopting an heuristic it provides a route to “the eventual discovery of
a strategy” (Beer, 1981, p. 55). We cannot know the future and as a consequence cannot
work out a strategy in advance but what we should do instead is to devise a system of
control that enables us to learn and modify its unwanted effects. Beers point made in
another context, is that our concern is to link a high variety input with a high variety
output (Beer, 1981, p. 53) and as a consequence we have to find ways in which we can
reduce variety. We suggest it is possible to produce a description of the general direction
in which a given subject is likely to move and to provide a means of assessing the effect
of the actions taken. However, the complexity of the situation means that modelling it is
not a straightforward application of a formula.

3.1 Surveillance and privacy
The challenges in understanding and modelling privacy are primarily two-fold. The
first challenge relates to developing a definition of privacy; an exercise which is
difficult because of the “incompatible” and rich characteristics of privacy. Brunk (2002)
said that “[P]rivacy is a matter of intellectual and philosophical thought and retains
few tangible characteristics, making it resistant to simple explanation”. As such,
finding an objective and universally accepted definition of privacy could be argued to
be a futile exercise (Klopfer and Rubenstein, 1977); in fact Odlyzko (2003) goes further
by speculating that the privacy problem is intractable.

The lack of a clear definition of privacy within the literature means that it becomes
necessary to adopt one which has resonance with the underpinning thinking within
this research, namely that there should be a transparency about the level and type of
surveillance used. In this sense we subscribe to Westin’s (1967) definition summarised
as the ability of an individual to control the terms under which personal information is
acquired and used. Westin’s definition is appealing because it associates privacy with
the user, rather than the environment. That is it relates to the user’s opportunities and
capabilities to protect the outflow of their personal information and private data.

The second point we make is that privacy seems to be interwoven with security in a
way that any study or treatment of privacy in isolation can result in misleading
conclusions. For example, when developing security oriented systems most Member
States of the European Union are careful not to ignore citizens privacy (see for example the
EC Directive 1997/66/EC of the European Parliament, 1997). In contrast in the USA,
the TIA project, which focussed on applying surveillance and information technology
to track and monitor “terrorists” was terminated by the Congress (Williams, 2006).
Following the terrorists attacks on the USA and EU the UK proposed the European passenger name record framework be expanded to increase the powers of data collection and use outside the air travel remit as a means of combating organised and serious crime. Clearly this is a complex problem with issues of security and personal freedoms interwoven in such a way that increasing one aspect may have a detrimental effect upon the other. Whilst accepting and the concerns of the UK Government about terrorist attacks on UK citizens and acknowledging the warning from the House of Lords (2008), we believe that it is important to provide a transparent system of control such that citizens are aware of what is happening and be assured that they are not over monitored. We believe that most citizens intuitively feel a symbiotic relationship between security and privacy such that the presence of one justifies the survival of the other. Our position, with specific caveats, is that:

- Privacy is dependent on security, as it cannot be claimed that privacy is achieved if there are no security mechanisms in place to protect it. Cryptography is an example of protecting confidentiality and of the dependence of security protecting privacy.
- Security is dependent on privacy with respect to demand; if there is no demand for privacy, some security controls will be deemed redundant and unnecessary. For example, if there is no requirement for anonymity in web browsing, then there will be no demand for anonymous proxies; or if the personal data are not required to be private then there would be no data confidentiality on the underlying data types.

The symbiotic relationship between privacy and security is not set in equal terms, but favours the latter because security can exist in some form without privacy. As Straub and Collins (1990) argued, the marginal advantage of security over privacy can be realised by the series of legislative controls introduced in a social system as an attempt to facilitate a break-even between these two concepts.

3.2 Modelling the situation

We do not claim this idea to be new as the work by Laudon (1996), Varian (1996), Huang (1998) and Posner (1978, 1999) sets a precedent which has led to research into the application of formal micro-economic techniques to analyse the threats that some security measures pose on privacy. Examples of research using micro-economic theory to gain insight into privacy has been published by Acquisty et al. (2003), Acquisti (2004), Otsuka and Onozawa (2001) and Ward (2000) in which privacy calculi were proposed – see for example Laufer and Wolfe’s (1977) “calculus of behavior” further promoted by Danev and Hart (2006).

Privacy is a human, socially driven characteristic and as such research into privacy metrics and calculi inherently involves human attributes such as perceptions and beliefs, demographic dependent data (Westin, 1996). For instance, Ackerman et al. (1999) place people into three distinct groups depending on their attitude to privacy, namely the privacy fundamentalists, the privacy pragmatists and the privacy unconcerned. Our view is that the application of a micro- or macro-economic ideas to study on privacy and security can only be meaningful if the sociological context is taken into consideration. Danezi and Wittneben (2006) demonstrate one such interdisciplinary type of research by applying social network theory to study the economics of privacy as influenced by mass surveillance.
Reductionist modelling methods of such complexity as the relationship between privacy and security is problematic as it is unquantifiable. But within the context of an economic analysis, avoidance of such deficiencies that are inherent in reductionism can be achieved by moving from micro to macroeconomics. By adopting modelling methods from macroeconomics we are able to produce a model which is useful because it allows us to produce a model of situations where not all variables are known. The relationship between privacy and security is one such situation.

4. ID management versus ID assurance
Increasing numbers of individuals using internet services has resulted in a paradigm shift from an emphasis on business use to citizen and e-governance. Crosby (2008) points out the paradigm shift that has brought privacy obligations to the foreground and disturbed the security agenda by requiring analysts to consider possibilities for migrating from ID management to ID assurance solutions.

Although ID management and ID assurance have common grounds they are two sides of the same coin. ID management depends on controls where both security and ID management support surveillance. ID assurance depends on security where both ID assurance and security support privacy.

The ID management versus ID assurance contrasts are reflected and analysed. In a project commissioned by the UK Government Crosby (2008) explored how an ID management solution could be developed and used by private and public sectors in the UK which would be of benefit to them and citizens. The study was carried out involving over 100 organisations with and individuals being consulted from all sectors and sizes of companies. We have adopted Crosby’s as a main point of reference in this research for the following reasons:

- it was conducted at a level appropriate to the research requirements of this paper (i.e. on an aggregate or macro level);
- it acknowledged the wider international context and as such the findings can have a wider remit; and
- the outcome of the study identified the purpose and context of the two schemes (ID management and assurance) in relation to the needs of surveillance and data collection.

The researchers had no control over the study and its conclusions and its contents are open for independent analysis.

4.1 Methodology
Macroeconomic theory is used to deal with ill-defined problems. For example, consider the functions of supply and demand which are used to define a product or service market. The underlying market can be viewed as an open or general system in which not all relations and variables can be accounted. Macroeconomic theory allows the introduction of assumptions that transfer the problem to a partial system. In economics this is the so-called ceteris paribus assumption, or all things being equal, under which levels of specific variables are considered fixed or constant (Schlicht, 1985). Such analysis will provide a snapshot of the problem so in order to give due consideration to the decision making process it is necessary to have means of relaxing the assumption in a controlled way to allow the study of certain scenarios. Relaxing is done when we introduce...
assumptions in the model which affect some of the controlled variables in “predictable” or generally acceptable ways. For instance, an increase in price of a product is expected to have a negative impact on the sales of that product. In a similar way, we might expect that an increment of surveillance technologies to have a negative impact on privacy.

To illustrate this point if we plot the aggregate quantity demand of, say, housing against price we would notice an inverse relationship between price and quantity demanded: the higher the price of a house, the lower the quantity demanded. From a macroeconomics perspective, the relationship between these two variables contains a plethora of other hidden variables. In order to draw the line or curve of quantity demanded versus price we consider all other variables as constant. By assuming that the level of one of the hidden variables changes — say the interest rate — we can establish a shift of the curve; the direction of the shift will be dictated by the sign of change of the interest rate (positive or negative).

We will now extend our argument to see what effect this might have on the relationship between privacy and security technologies. We present the two alternatives offered by Crosby which are compared to the current situation, a mosaic of different systems containing a plethora of personal data, as elaborated below. This is followed by a systematic application of the proposed methodology which invokes an isomorphy of macroeconomic theories and tools.

4.1.1 Baseline case: “many eggs in many baskets”. There is no national ID card scheme in the UK. There are many strategies and solutions for both public and private sector for individuals to verify their identity, depending on the relevant requirements of the underlying industry (Crosby, 2008). For example, in banking opening a new account requires proof of identity which can take the form of a driving licence (or a passport) and a utility bill to the individuals’ home address, this process even applies to existing and new customers that wish to open a new savings account. Telephone or on-line banking transactions require the customer to provide a series of answers to obscure questions such as mother’s maiden name or shoe size. To the average citizen such checks can be tedious but to the criminal of average intelligence falsifying an identity which would satisfy this level of enquiry is relatively straight forward. The Information Technology Association of America (ITAA White Paper, 2005) reported a growing level of identity theft and fraud and attributed this increase to the US system which makes it easy for criminals to obtain false identities. The report points out the ease at which it is possible to gain an identity providing a startling example that:

Identity thieves need not always go to the trouble of trying to craft their own phony identities. Sometimes they can simply purchase the documents by bribing department of motor vehicle personnel (ITAA White Paper, 2005).

In the public sector once a (temporary) national insurance number has been obtained then an individual can begin to access a variety of state benefits and also have an identity that will satisfy most other institutions. In each of these instances records will be created for individuals who are ostensibly protected by the UK 1998 Data Protection Act which forbids the exchange of data between separate agencies.

The above situation results in the creation of disparate systems where some hold incomplete and potentially conflicting data as well as overlapping and redundant entries. Such a situation will produce an assortment and a multitude of ID management and ID assurance systems. Not surprisingly an attempt to develop interfaces between
all these different systems is a non-trivial task. For example, in order to operate many
public sector agencies frequently circumvent their lack of interface by inventing
“simple” yet risky procedures such as the “Frisbee Network” of CD exchanges (BBC,
2007; Collins, 2007).

4.1.2 ID management: “many eggs in one basket”. The principle behind ID
management is to increase the amount of information collected for every citizen
(Crosby, 2008). Information is held for the purpose of protecting society from fraudulent
behaviour, criminal activities, and terrorism (Wang et al., 2002). ID management is
about the unreserved collection of data, which includes identification as well as
behavioural data. This will have an impact to security as Straub (1990) demonstrated
empirically that active monitoring of an information system is indeed a deterrent to
computer abuse. The practical implication of this principle requires surveillance
technologies to be implemented and coordinated and results in a trade-off between
security and privacy. The result is an increase in the level of complexity and cost
because by storing a plethora of personal data much will fall into special legislative
categories, high confidentiality. Ways of manipulating, handling, processing and
combining the data will also add to the complexity of its management. For a complex
system to be manageable it is necessary that the flexibility of the system and controls
will be reduced (Lucas and Olson, 1993). We are reminded that “[…] every real machine
embodies no less than an infinite number of variables” (Ashby, 1960, p. 15). In other
words the controller must be capable of responding with as much variety as the affects
of a changing environment has upon the object to be controlled. In order to model any
system we have to simplify and ignore all but a few of its variables which means that
the designer will effectively define an abstract system based upon their perception of
the systems requirements.

Potentially ID management creates a single point of failure, because if data mining
is applied the data could be accessible by unintended parties or authorities. Inference
control is an issue in many dimensional databases (Wang et al., 2004) because if the
data are available then they can be used for other than the intended purpose of
managed citizen identification. Security technologies focus on meeting the goals of
prevention, protection and recovery (Bishop, 2002) but the latter two do not contribute
to the goal of preserving privacy. Privacy is preserved when information about a
person is only disclosed to a specific group of entities (or subjects), and is one failure
which results in unauthorised disclosure of information. When dealing with a
centralised repository of data the problem of unauthorised disclosure becomes even
more challenging than providing a set of access control mechanisms because of the
data inference problem, i.e. data leaking information about other, higher classified data.
Challenges to privacy and security in this case is represented as an inference control
problem (Sweeney, 2002).

4.1.3 ID assurance: “an egg per basket”. The fundamental difference between an ID
management and an ID assurance system is that the latter intends to support the
development of a trusted system for identity verification. This is achieved through
minimizing the amount of data held on each citizen, thus supporting privacy. The data
itself is of low confidentiality as the data relate only to identification and not behaviour.
As a direct consequence surveillance is not required and privacy is supported. Because
of the relative limited scope, amount and confidentiality of the data, security
requirements will be less complex and less expensive.
5. Applying the methodology
First, we consider those security controls that aim to protect privacy. In this context we use the term security technologies in a generalised fashion to encompass all types of security controls, both technical and organisational. Accordingly we adopt an aggregate view by splitting the security technologies into two markets namely, the defensive security market and the adversarial security technologies market. The defensive security market consists of all those technologies which are used to protect privacy in a defensive manner. These are typically access control techniques involving services such as identification, authentication, authorisation and accountability. From a practical perspective these services can be implemented by defensive security technologies such as cryptography, firewalls, intrusion detection systems, anti-virus software and biometrics. Adversarial technologies consist of all those technologies which are used proactively to audit the defensive security controls. Examples of adversarial technologies include security scanners, vulnerability and penetration testing tools.

The distinction we make between the two categories relates to purpose and intention. For the purpose of this research we assume that defensive technologies are used solely for benign purposes, but adversarial technologies can be used for both benign or malicious purposes. An example of a benign use of adversarial technologies is ethical hacking which is normally found within the kernel of a security assessment exercise. We emphasise that both defensive and adversarial security technologies are required for protecting privacy. For example, removing ethical hacking would render privacy protection mechanisms incomplete and eventually ineffective.

5.1 Initial case: an aggregate view
Advancing Katos and Patel's (2008) argument we consider the current situation of many types of user identification systems with varying degrees of interfacing designed to meet a range of security requirements some of which may be conflicting or incompatible. The data are dispersed throughout these user identification and authentication systems. As such pieces of data may be overlapping, redundant, incomplete and conflicting. Within this mosaic of data and security requirements we identify pairs of relationships between certain variables. Specifically, the following assumptions are made for the two markets (Katos and Patel, 2008).

A. Security technologies market

- **Security demand versus price.** Security technologies are seen as economic goods. The aggregate demand (SD) of these technologies depends on their price (P). The demand for security technologies is represented by a monotonically decreasing function \( SD = f(P) \), i.e. the lower the price of security technologies (P), the higher the demand of security technologies (SD) creating an inverse relationship between quantity demanded for security technologies and price.

- **Security supply versus privacy.** The new economic analysis of privacy offers arguments to those who believe that individuals make an effort to act rationally (Inness, 1992) and choose whether to adopt privacy technologies. We assume that security is required in order to have privacy, because privacy cannot exist without security. In this case the supply for security technologies function \( SS = g(V) \), says the more important (higher) privacy (V) the greater the quantity of security technologies (SS), i.e. there is a positive relationship between supply...
of technologies and privacy. It is important to note the form and shape of security here because privacy is bounded by the supply of the security technologies, but security also depends on privacy such that if privacy disappeared, the portion of security technologies dealing with enhancing privacy would also disappear. In other words we argue that there is a symbiotic relationship between security and privacy with some advantage allocated over security. Removal of privacy would not necessarily result in a collapse of security, but it is likely that the latter would exist in a different form (e.g. a totalitarian or dictatorial regime).

- **Security supply versus security demand.** Branson and Litvack (1981) and Dornbush and Fischer (1998) suggest that market forces and economic laws, if left alone, will eventually push security technologies demand to equilibrium with security technologies supply, regardless of their initial allocation. This is represented by the identity function $SD = SS$, or $f(P) = g(V)$.

The model in Figure 1 is constructed by chaining the three pairs of relationships presented above in a way that an equilibrium – or relationship – between price and privacy satisfies (adapted from Branson and Litvack (1981)):

$$SD = SS$$

or equivalently:

$$f(P) = g(V)$$

where:

$f(P)$ = security technologies demand, with respect to price.

$g(V)$ = security technologies supply, with respect to privacy.

A change in prices of $\Delta f$ will change the left-hand side of equation (1) by $\Delta P \cdot f'(P)$. Similarly, a change in privacy of $\Delta V$ will change the right-hand side of equation (1) by $\Delta V \cdot g'(V)$.

![Figure 1. Security technologies market](image-url)
Therefore, from \( \Delta P \cdot f'(P) = \Delta V \cdot g'(V) \) we obtain the slope of the SD-SS curve (which represents the security technologies market) as:

\[
\left. \frac{\Delta P}{\Delta V} \right|_{SD-SS} = \frac{g'(V)}{f'(P)} < 0
\]

The slope is negative because \( f'(P) < 0 \) and \( g'(V) > 0 \).

**B. Adversarial technologies market**

A fundamental distinction between security and adversarial technologies, is that in the latter there needs to be a distinction based on the intention or purpose of the technology –, i.e. is it benign (for protecting privacy), or malicious (for defeating privacy)?

- **Benign adversarial technologies demand versus privacy.** The privacy-enhancing adversarial technologies demand (or equivalently the technologies used for benign purposes, SB), depends on the level of privacy intended. The aspect of good uses of the adversarial technologies relates to privacy as follows; the higher the level of privacy (V), the more security systems may be demanded in order to keep privacy at this high level. Thus, there exists a positive relationship, indicated by the function \( SB = k(V) \).

- **Malicious adversarial technologies demand versus price.** The demand for malicious purposes adversarial technologies is represented by the monotonically decreasing function \( SM = h(P) \) which depicts the fact that the lower the price of security technologies (P), the higher the quantity demanded of security technologies for malicious or fraud purposes (SM) and thus, there exists an inverse relationship between quantity demanded for fraud purposes security technologies and price.

- **Aggregate demand for adversarial technologies.** Summing the two components of the security technologies demand, we have the demand function for security technologies: \( SD = SM + SB \) or \( SD = k(V) + h(P) \).

- **Aggregate supply for adversarial technologies.** The supply side of adversarial technologies is determined in the short-run by technological factors in the economy and thus it is considered to be exogenously fixed at the level \( SS^* \). Equating the security technologies demand to the exogenously fixed supply of security technologies gives us the equilibrium condition: \( SS^* = SD \), or \( SS^* = h(P) + k(V) \). Simply stated, the security technologies for malicious purposes demand and the privacy-enhancing security technologies demand is equal to the exogenously given supply of security technologies.

As with the security technologies market the pair relationships denoted with the above assumptions are formally described by considering the supply to be equal to the demand of adversarial technologies which is the sum of the demand of adversarial technologies used for benign and malicious purpose:

\[
SS^* = SB + SM,
\]

or:

\[
c = k(V) + h(P)
\]
where:

\[ h(P) = \text{technologies demand for malicious purposes, with respect to price.} \]

\[ k(V) = \text{technologies demand for benign purposes, with respect to privacy.} \]

\[ c = \text{total quantity of technologies available.} \]

A change in price of \( \Delta P \) will change the right-hand side of equation (2) by \( \Delta P \cdot h'(P) \). Similarly, a change in privacy of \( \Delta V \) will change the right-hand side of equation (2) by \( \Delta V \cdot k'(V) \).

Since the left-hand side is fixed, the changes in the right-hand side must add to zero for equation (2) to remain satisfied:

\[ 0 = \Delta P \cdot h'(P) + \Delta V \cdot k'(V) \]

Thus:

\[ \frac{\Delta P}{\Delta V}_{SM-SB} = \frac{k'(V)}{h'(P)} > 0 \]

The slope of SM-SB curve in Figure 2 describing equilibrium pairs of P and V, represents the adversarial technologies market and is positive because \( h'(P) < 0 \) and \( k'(V) > 0 \).

So far we have derived two pieces of geometric equipment. One gives the equilibrium pairs of P and V in Figure 1, i.e. the SD-SS curve in the security technologies market and the other gives the equilibrium pairs of P and V in Figure 2, i.e. the SM-SB curve in the technologies of the adversary market. By placing these two curves in the same quadrant, shown in Figure 3, obtained by solving the two equilibrium equations \( f(P) = g(V) \) and \( SS^* = h(P) + k(V) \) simultaneously, we can find the single P, V pair that gives equilibrium in both markets. This is shown as the equilibrium point \( (P_E, V_E) \) of the intersection of the SD-SS and SM-SB curves in Figure 3.
C. Summary

At this stage the above exercise is incomplete for two reasons. First, as with most qualitative variables there is no acceptable metric for privacy. Privacy being equal to PE has limited meaning or substance as there is no objective metric for privacy. Yet it is implicitly accepted by developing this approach that privacy could be captured by an ordinal variable agreeing with the wider consensus that certain actions may reduce or increase privacy, despite not being able to quantify the precise changes. An indicative example revealing the ordinal scale of privacy is the true statement: “Privacy will decrease if ISPs are legally allowed to monitor their customers’ internet browsing actions and share this information with any third party”. Second, the assumption of ceteris paribus means that the model exhibits a snapshot of a market or environment so we are transforming a general to a partial system by making the levels of all other variables constant.

Nevertheless, the added value of this model is in its ability to allow the ceteris paribus assumption to be relaxed by accommodating changes to existing or introducing new assumptions. By doing this we can run what-if scenarios and track the relative changes of the qualitative variables such as privacy. It is this feature that makes feasible validating statements like “privacy decreases if the population of CCTV cameras increases”, hence avoiding the need for employing quantitative and strict metrics for privacy. We recognise that it will be infeasible to show the order of change of a variable (i.e. show how much privacy would decrease for example); but this is not the purpose of the model and the underlying methodology and as assumed earlier a rational measurement is not valid on an ordinal variable. The output of the model is the recommendation of hypotheses that will create further empirical research activities. The validation of the model was undertaken through the use of a publically accessible scenario chosen because its known outcome provides a point of reference and a pilot study.

We now return to the two policies of ID management and ID assurance and assess their impact through the use of the proposed methodological approach.

5.1.1 Comparative statics exercise: ID management. In ID management an abundance of personal data is collected centrally which is controlled by a limited and
select group of individuals or organisations. Comparing this policy to the base case, we can make the following observations:

M1. As all data will reside in one system, the complexity of the system will increase. The larger data schemas will result in a larger number of permutations of states, data and interfaces accessing the system. Reflecting upon Ashby’s LRV shows this will result in a larger number of controls. In order to maintain the same amount of privacy as before, more security will be required.

M2. With “all eggs in one basket”, the data type with the highest privacy requirements is likely to set the security requirements of the overall ID management system.

M3. Increased complexity of the ID management system means security will become more expensive and, assuming a fixed budget, aggregate demand will appear to drop.

M4. Some security technologies will be available to a limited, select group.

Assumptions M1 and M2 would cause a leftward rotation of the privacy-security supply curve in Q4, as shown in Figure 4. Assumptions M3 and M4 produce a rightward shift of the demand curve, shown in Q2. The movement of the curves in Q2 and Q4 would have a knock-on effect to the relationship between privacy and price in Q1, by causing a leftward shift. The new equilibrium function is represented in Q1 in Figure 4 by the dashed line SD’SS’. The new position of the equilibrium function is definitely to the left of the initial position, because the effects of the changes in the security technologies demand and supply functions are reinforcing one the each other.

Accepting the predicted outcome from the model we expect an ID management solution is expected to affect the adversarial market as follows:

Figure 4. The impact of the introduction of a central ID management system to the security technologies market
M5. In line with M1, additional auditing or use of adversarial technologies for benign purposes would be required in order to maintain privacy to a certain fixed level.

M6. The value of the equivalent database holding the vast amounts of personal biometric and biographical data will be substantially higher than any smaller system containing a subset of the data. Therefore, the demand for adversarial technologies for malicious use would increase, as the target system would be appealing to attackers.

Assumption M5 would influence accordingly by a leftward rotation of the privacy – benign adversarial technologies relation shown in Q4. Assumption M6 would cause a leftward shift of the demand curve in Q2, since for a fixed price there will be a higher demand of malicious use of adversarial technologies due to the higher potential gain of compromising the system. These assumptions are reflected in Figure 5, where the security technologies curves are superimposed in Q1 to show the new market equilibrium E'.

Comparing points E and E' (comparative statics) it is seen that privacy decreases from $V_E$ to $V'_E$, whereas the price seems to remain relatively stable. Intuitively, this could be explained by arguing that any attempt to reduce the price by trading off privacy is “compensated” by a response – increase – in adversarial systems used for malicious purposes. At an aggregate level we observe a drop in privacy with no benefit to price.

From the analysis above we can observe that the changes can be established for one parameter (in this case privacy) whereas for the other parameter (that is, price) the actual curves need to be estimated in order to reach a formal conclusion. In either case the comparative statics estimation can be derived by solving the simultaneous equations for the changes caused by the discrepancies introduced by the exogenous variables to determine the new equilibriums. An example is provided in the Appendix.

---

Figure 5.
The impact of the introduction of a central ID management system to the adversarial technologies market.
5.1.2 Comparative statics exercise: ID assurance. The ID assurance scenario shows a minimum amount of data stored in the ID verification system, but also that this data would be of a low value in terms of confidentiality and usability. We could view the system as a public directory of high integrity requirements. In an ID assurance system, the following assumptions may be drawn:

A1. Overall, there are significantly less data than the other two user identification systems presented earlier, particularly due to the fact that no behavioural data would reside in the system.

A2. The citizens are seen as active and effective parts of the security processes largely through the high frequency of use of the system (Crosby, 2008).

A3. The overall complexity of the system will be reduced, as the confidentiality requirements would be low.

Assumptions A1-A3 would effectively cause the security technologies market to exhibit a higher amount of privacy for a certain level of supply of security technologies. That is, given a certain supply level of security technologies, privacy is expected to be higher in this scenario, since the volume and confidentiality of the data will be less than in the base case. This would result in a rightward rotation of the privacy versus security curve in Q4 in Figure 6. Moreover, assumption A3 would result to a rightward shift of the security demand versus price curve in Q2 in Figure 6, since the aggregate demand for security technologies is expected to drop (there will be fewer data and less complex systems to protect).

From the resulting shift of SD-SS curve in Q1 it can be seen that there is no significant or clear-cut movement of the privacy versus price curve. The decrease in demand of the security technologies (Q2) compensates any clear gain in privacy (Q4). With respect to the adversarial technologies market, the following assumptions are made:

![Diagram](image)
4. In line with A3, a lower complexity would in turn require smaller security auditing efforts in order to maintain a certain level of privacy.

A5. The ID assurance system would be of a lower value to attackers and a less attractive target. As such, we argue, that the demand of adversarial systems for malicious purposes would drop.

Assumption A4 would cause a rightward rotation of the privacy versus benign adversarial technologies curve in Q4 in Figure 7. Assumption A5 would be reflected in the model as a rightward shift of the demand curve in Q2. The consequences of the combined shifts of the two curves to the privacy versus price curve in Q1 are shown as a distinct rightward shift. The security technologies curves are superimposed in Q1 to show the new market equilibrium E’.

Comparing points E and E’ it can be seen that there is a clear increase in privacy and a decrease in price. Intuitively this outcome seems correct, since there will be less security systems required to protect reduced data sets for a specific purpose (identity verification) and consequently of a limited value to an attacker. If the data are mainly unclassified or have low confidentiality requirements, privacy threats would be out of context. This is due to the decoupling of the ID assurance system from confidentiality needs. However, the integrity requirements would remain high, as unauthorised modification of the relatively few user identification data types would be a valid threat for the identification system.

6. Conclusions
In this paper the relationship between security and privacy was considered from an aggregate perspective. By observing the shift from monitoring to surveillance and from

![Figure 7. The impact of the transition to an ID assurance system to the adversarial technologies market](image-url)
the business employee to the citizen (now an end-user of e-government) we have embraced a key idea from general systems theory namely the belief in the possibility of an “isomorphy of concepts, laws and models in various fields” (Schoderbek et al., 1990, p. 35). To this end we incorporated the ideas from the cross methodology from macroeconomics as a means of investigating the relationships between privacy security based upon cost and consumption. Specifically we considered security and privacy to be economic goods and as a consequence price functions were attached to them.

Taking into account Ashby’s LRV we argue that excessive surveillance will not solve security issues as the level of threat and intensity is not constant and was unpredictable. Two alternative scenarios or “futures”, namely ID management and ID assurance were considered using scenarios taken from a publicly available report. This report had been commissioned by the UK Government and provides the reader with a rich source of research. Using the model our analysis showed that ID management, characterised by the unreserved and centralised collection of citizen’s data, offers no perceived benefits to security, but the level of privacy will decrease with no significant price trade-off. In other words there will be less privacy for the same price and as a consequence privacy would be relatively more expensive. In security terms we do not expect improvement either, as a centralised repository of personal data will raise the complexity of the user identification system and the security controls and increase its attractiveness to malicious adversaries because of its added value.

In the case of ID assurance we have an identity verification system with a minimal amount of data exhibiting low confidentiality allowing participation of the end-users – stakeholders – through high frequency of use. Such an identification system will have low complexity. Our analysis showed that privacy will increase at a lesser price. This is not surprising because the ID assurance system would not only be of low value to attackers, but also the security employed would serve more privacy and less surveillance since user identification would depend on the integrity rather than the confidentiality of unclassified data.

In the paper the analysis was undertaken by introducing a series of assumptions for each of the scenarios. Whilst the validity of the assumptions and the outcomes of the study can be verified by empirical means the level of analysis has the benefit of not relying upon a stereotype population. For example, there is no need to take into account the privacy pragmatists, fundamentalists and the unconcerned which is usually a consideration in empirical research. We do recognise that there may be a socio-economical environment where these assumptions may not hold but this is an acknowledged feature of macroeconomics as Beer (1981) reminded us that it is not possible to fully specify a complex situation. “The strange thing is we tend to live our lives by heuristics and try to control them by algorithms” (Beer, 1981, p. 53). We accept that by porting the tool into the privacy and security domain our analysis and findings will be affected in a similar way but with such complex problem spaces which contain unknown variables it is beneficial to have such a model that is capable of producing hypotheses and one that can verified empirically. The results of this initial research has provided an encouraging first step in finding a practical and systemic way of assessing the use of technologies for surveillance and balancing these against the impact upon the individual right to privacy.
References


Macroeconomics of privacy and security
Further reading


Appendix

The following discussion is in accordance to the analysis by Branson and Litvack (1981) for deriving the general multiplier to measure the discrepancy or change when relaxing the ceteris paribus assumption. Consider an exogenous variable causing a shift on the DS curve as shown in Figure A1. Equilibrium values of the price and privacy are determined by the intersection of the DS and MB curves. Shifts of these curves create a discrepancy between DS and MB at the old equilibrium point. For example, if \( E_1(P_1, V_1) \) had been an equilibrium, a shift from \( D_1S_1 \) to \( D_2S_2 \) will create a discrepancy of \( V_3 - V_1 \) at \( P_1 \) after the shift.

Considering that:

\[
\frac{P_2 - P_1}{V_2 - V_1} = \frac{\Delta P}{\Delta V}_{MB}
\]

the change in equilibrium privacy can be expressed as:
We can express $P_2 - P_1$ in terms of the shift $V_3 - V_1$ as follows. We know that:

$$V_3 - V_1 = (V_2 - V_1) + (V_3 - V_2),$$

where:

$$V_2 - V_1 = \frac{P_2 - P_1}{\Delta V_{MB}}$$

and:

$$V_3 - V_2 = \frac{P_2 - P_1}{\Delta V_{DS}}$$

Therefore:

$$V_3 - V_1 = \frac{P_2 - P_1}{\Delta V_{MB}} \cdot \frac{P_2 - P_1}{\Delta V_{DS}} = (P_2 - P_1) \left[ \frac{1}{\Delta V_{MB}} - \frac{1}{\Delta V_{DS}} \right]$$

$$= (P_2 - P_1) \begin{bmatrix} \frac{\Delta P}{\Delta V_{MB}} & \frac{\Delta P}{\Delta V_{DS}} \\ \frac{\Delta P}{\Delta V_{MB}} & \frac{\Delta P}{\Delta V_{DS}} \end{bmatrix}$$
and:

\[
P_2 - P_1 = \frac{\Delta P}{\Delta V_{MB}} \frac{\Delta P}{\Delta V_{DS}} (V_3 - V_1)\
\]

The change in equilibrium privacy, then, for a shift in DS can be expressed as:

\[
V_2 - V_1 = \frac{\Delta P}{\Delta V_{DS}} - \frac{\Delta P}{\Delta V_{MB}} (V_3 - V_1) \quad (A1)
\]

If now the MB curve had shifted from one that passed through \(E_0(P_1, V_3)\) to the one shown with the \(D_S2\) fixed, a similar process would lead to:

\[
V_3 - V_2 = -\frac{\Delta P}{\Delta V_{MB}} (V_3 - V_1) \quad (A2)
\]

Equations (A1) and (A2) differ only in the numerator term. Substituting into equation (A1) the slope formula we derived earlier, we have:

\[
V_2 - V_1 = \frac{(S'(V)/D'(P))}{(S'(V)/D'(P)) + (B'(V)/M'(P))} (V_3 - V_1)
\]

Considering an autonomous change in \(D = D(P)\), say by \(\Delta a\), then we will have:

\[
V_3 - V_1 = \frac{1}{S(V)} \Delta a \quad (A3)
\]

Substituting equation (A3) above we get:

\[
V_2 - V_1 = \frac{(S'(V)/D'(P))}{(S'(V)/D'(P)) + (B'(V)/M'(P))} \cdot \frac{1}{S(V)} \cdot \Delta a
\]

or finally:

\[
V_2 - V_1 = \left[ \frac{1}{S(V) + ((D'(P) \cdot B'(V))/M'(P))} \right] \cdot \Delta a
\]

The term in brackets is the multiplier for an autonomous shift in the security technologies demand. Similarly the multiplier for the security technologies supply can be derived.

**About the authors**

Vasilios Katos is Assistant Professor of Information and Communications Systems Security at the Department of Electrical and Computer Engineering, Democritus University of Thrace, Greece. Prior to his current post he was Principal Lecturer at the School of Computing, University of Portsmouth, where he participated in the development of the interdisciplinary Master’s course, MSc in Forensic IT. He has worked in the industry as a security consultant and expert witness in information systems security. His research interests are in information security, privacy, digital forensics and incident response. Vasilios Katos is the corresponding author and can be contacted at: vkatos@ee.duth.gr
Frank Stowell is Professor of Systems and Information Systems at the University of Portsmouth, UK. Before moving to Portsmouth he was Director of Campus at De Montfort University at Milton Keynes. He has a PhD in Organisational Change and is an expert in Systems Thinking and Practice. He has published papers and texts in the field and presented papers at a number of international conferences in Europe and the USA. He has supervised a number of research projects and continues to supervise and examine PhD research. His latest publication is *The Manager’s Guide to Systems Practice* (Wiley, 2012). He has been a specialist reviewer for the Quality Assurance agency for Higher Education within the UK. He is chair of the Systems Practice for Managing Complexity associates, past President of the UK Academy of Information Systems and the UK Systems Society (www.ukss.org.uk/). He is the current chair of the Council of Information Systems Professors. Prior to his academic career he was a consultant in a central government-sponsored Management Systems Development Group and has experience of defining and developing IT-supported management information systems. His area of interest is in the application of systems ideas to the development of IT-supported information systems. His present research is in the development of ways in which the client can lead and control the development of their information system.

Peter Bednar is a Researcher in Informatics at Lund University in Sweden. He is also a full-time Senior Lecturer in Systems and Information Systems at the School of Computing, University of Portsmouth, UK. Having an engineering background, he worked in several highly competitive industries prior to his academic employment. His research interests are in information systems, information security, contextual analysis, systemic uncertainty and ambiguity.