Jentzsch, Nicola

**Research Report**

# What Is Special in the Economics of Cybersecurity and Privacy?

IPACSO White Paper, No. 2

IPACSO White Paper

# What is Special in the Economics of Cybersecurity and Privacy?

by Dr. Nicola Jentzsch

October 2015

# Abstract

One of the most popular questions in information security economics is whether there are any special features relating to privacy and cyber-security products and services that separate these from traditional goods, like apples or cars. This paper is a contribution to this discussion. First, different goods and services are compared to assess whether privacy and cyber-security are *in fact* different. Although basic, it is enlightening. We then discuss how economics treats key features and whether the observed differences justify any 'special' terminology.

## IPACSO White Paper No. 2 (October 2015)

This White Paper is produced as part of the Innovation Framework for Privacy and Cyber Security Market Opportunities (IPACSO). It draws partially on the material in the Reports D4.1 and D4.2A (downloadable at www.ipacso.eu). The author thanks Aidan Kenny and Mark Cerolan for valuable comments. The content does not reflect the opinion of DIW Berlin as institution or IPACSO as a consortium, but the author's own assessment. Comments and suggestions are welcomed.

## Corresponding Author

Dr. Nicola Jentzsch, DIW Berlin, Mohrenstr. 58, 10117 Berlin, T. +49 30 89789-234, F. +49 30 89789-103, njentzsch@diw.de

# Table of Contents



# List of Figures



# List of Tables

# I. Introduction

Are there any special features relating to privacy and cyber-security that make these products and services special? This is a question frequently asked at international cyber-security and privacy conferences. While it seems basic at first sight, it is a rather tricky question. Why? Because first one has to determine what 'special' means. The Oxford Dictionary holds that special means 'better, greater or otherwise different' from the usual. So the least we can say is that privacy and cyber-security goods and services should differ from traditional goods and services in several key aspects.

An affirmative answer to the 'special' question implies that these features *potentially introduce different competitive dynamics and market outcomes*. In this case, we would need new economic models in order to explain observed market developments and we would need new (competition) policy instruments to effectively regulate markets. Moreover, **more and more products and services will become identity related** – this trend is becoming even more pronounced with the increasing deployment of Big Data technologies and analysis.

One path of reasoning is to simply compare privacy and cyber-security goods and services with traditional ones such as apples, cars, insurance or other information goods (such as music CDs). In the past, others have also conducted comparisons of information goods with traditional goods (see Shapiro and Varian 1999). However, we focus on privacy and cyber-security, which will be further explained in the second chapter.

This paper also mentions a number of models that already exist in economics for dealing with some of the challenges associated with the special features of cyber-security and privacy.

**Note that this is not an academic paper**, but an introduction that presents some key insights from economics to a wider audience interested in the discussion about 'special features' of privacy and cyber-security.

# II. COMPARING APPLES, CARS AND SECURITY

Goods (and services)[1] have features that influence their tradability. Tradability, in turn, impacts the competitive strategies of firms. Moreover, the features of goods also impact the willingness to pay for them. Thus, one needs to examine the individual features of goods in order to obtain insights into the competitive dynamics in markets for personal information.

At the most basic level, there are **traded and non-traded goods**. Apples, cars and music CDs are examples of traded goods, whereas human kidneys and other organs as well as air are non-traded goods. All of the aforementioned do not need to be explained. However, before we elaborate on the specific features of the goods under scrutiny, the terms of **cyber-security, personal information and privacy** need to be explained as they have different meanings in different contexts.

## 2.1 BASIC CONCEPTS

In line with different international definitions of **cyber-security,**[2] the term refers to all measures with the primary purpose of establishing, preserving, and increasing the integrity and availability of information systems as well as the authenticity and confidentiality of their content. Schechter (2004) defines security as "process of protecting against injury or harm." It is important to note that security can be a process as well as a condition, the latter denotes as situation free of harm.

Therefore, we can think of **cyber-security as a condition**, which is to be achieved with **hardware, software and services** that serve the primary purpose of achieving that condition.

The **cyber-security market**, thus, can be defined as a physical or virtual place, where demand and supply for cyber-security products and services meet. The

[1] Except where explicitly noted, these terms are used interchangeably in the following.

[2] Definitions have been published in the past by European Commission, Eurostat, the ITU, as well as governments of the U.S., United Kingdom, France and Germany, among others.

market is different from the industry. The term '**cyber-security industry**' defines the supply side of this market.

**Cyber-security products essentially establish a promise**, the promise of a condition free of harm (disruption or manipulation). In order to buy such products and services, a buyer needs to trust the seller (**trust endowment**). Such endowment is difficult to obtain, but easy to destroy and very hard to restore.[3] This holds especially in the environment of information business, because information is **extremely hard to control and safeguard**. The latter is the very reason for the existence of the cyber-security industry.

Note that for now, no statement has been made with respect to whether cyber-security goods and services are special when compared to traditional goods and services.

**Personal data,** defined according to the concept set out in the European Data Protection Directive EC/46/95,[4] is traded in different forms. Examples include credit reports, marketing profiles, and self-tracking products. Personal information constitutes a **signal about observable and unobservable characteristics** of an individual relating to their preferences, willingness to pay, and switching flexibility; all of which are often not directly observable. Firms are interested in observing these non-observables. Identity information might not be necessary in this case. However, techniques such as behavior-based pricing and product personalization require the identification of individuals, either via their natural identity or with a token, in order to compile a history.

There is no internationally accepted definition of **personal privacy**. As discussed elsewhere, personal privacy arises with an asymmetric distribution of personal information between market participants, where one side *privately holds personal information* (Jentzsch 2015). There is much confusion around whether privacy can be traded.[5] However, what is essentially meant by the term 'markets for privacy' are markets for privacy-enhancing products and services.

The key feature that separates personal data products from other products and services is the identification of the individual as a production input (see Table 1).

[3] Note that the trust endowment is nothing special. In order to purchase a car, a buyer needs to be sure that it is safe.

[4] As a reminder, personal data in the Directive is defined as meaning "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[5] See, for example, Cohen, J. (2012). Irrational Privacy? Journal on Telecommunication & High Technology Law,

Personal identification is not required for what I call pseudonymity and anonymity products (such as anonymization websites).

Note that these goods are often grouped together under the header 'privacy products', but they work quite differently. The three product categories are information goods. However, they differ in the key production input needed, i.e. whether personal information is provided or not, in order to provide them.

Consider the de-personalization products in Table 1. These do not require any personal identity information as input. Pseudonymity products shield the natural identity of a data subject to a certain extent through the deployment of quasi-identifiers or tokens, such as random numbers, IP-numbers, etc.

Personalized products, on the other hand, can be found at the other extreme of the range: here personal information is the key input for the provision of the good or service. The three categories can be summarized under the header '**privacy goods and services**.' The examples made below will help to understand what is meant here.

**Table 1 Comparing De-personalization, Pseudonymity and Identity Products**

| | **Degree of Identification** | | |
|---|---|---|---|
| | **De-personalization Products** | **Pseudonymity Products** | **Personalized Products** |
| **Input** | No identification | Tokens, quasi-identifiers | Identification |

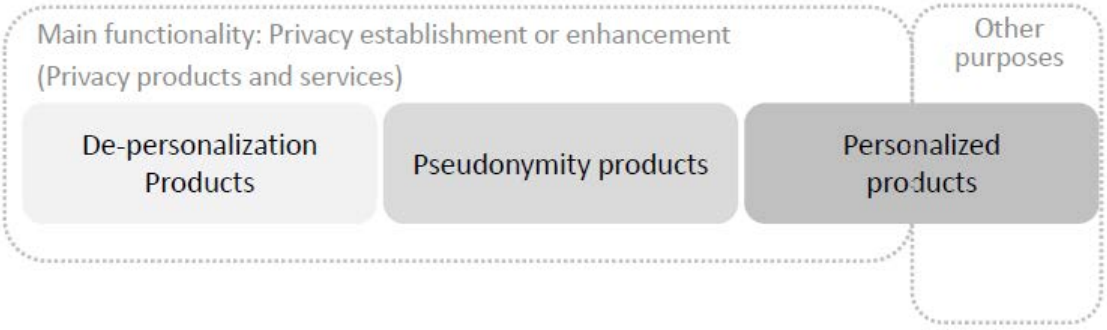
Based upon the above, we can state the market for the aforementioned products and services is a physical or virtual place, where demand and supply for these products and services meet, similar as above. The term '**privacy industry**' defines the supply side of this market.

We refer to privacy goods and services as those that have the **primary purpose (functionality)** of establishing, preserving, and increasing control, use and integrity of personal information. This means that data control is not a mere quality feature of the product, but its main functionality.

## Some Examples of Privacy Products and Services

We use several examples below to show how the categories differ from each other. Note that this is only a first step in developing a more thorough taxonomy of such products and services. Figure 1 gives a visual overview, which is explained below.

**Figure 1 Product categories in the Market for Privacy Goods and Services**




Privacy products essentially establish a promise, i.e., that information control can be increased. The first category is that of de-personalization products and services. The term 'de-personalization' owes to the fact that anonymization is very difficult to achieve. Research shows that it is almost impossible to establish anonymity, even in coarse datasets (de Montoye et al. 2013).

The category of **de-personalization products** includes all types of products with the main purpose of providing de-personalization to the user, such as online anonymizers.

**Pseudonymity products** include all products that assign a token or quasi-identifier to the data subject in order to provide pseudonymity. These, for example, come in the form of personal data vaults (that do not disclose identity information to the other market side) or shopping cards where the user is assigned a random number.

**Personalized products** are all products that require identifying information as product input. Note that these can either (1) serve the purpose of enhancing privacy, thus, belonging to the aforementioned privacy products group; or (2) they serve the *opposite purpose*, i.e. more personal information disclosure. An example for (1) is reputation management products that require identity information, but allow the individual to erase personal information on the Internet thereby increasing data control. These belong to the privacy product market.

An example for (2) is Jawbone UP, used by individuals for tracking their own fitness (e.g. the hours of exercise).

A credit report is also a personalized product, however individuals have very little control over its composition, except for – in many regulatory regimes – access and rectification.[6] It does not belong to the privacy product market.

A **narrow definition of the market** for cyber-security or for privacy products and services only refers to those products and services whose main functionality is the provision of cyber-security or privacy (e.g. Anti-Virus software).

A **wider definition** encompasses those products and services with the main functionality of security or control, but also products where the inherent qualities/ancillary features establish security and control (other software that includes a Firewall, where the latter is no stand-alone product).[7]

Note that the **immateriality** of information allows product versioning. This means that a product based upon one specific set of data just needs to include additional privacy-related product qualities (e.g. the FaceBook profile with and without privacy features turned on) to yield a product that belongs to a different product category.

## Cyber-security and Privacy Markets: Are they Different?

Privacy products and services belong to the cyber-security market in general. As a reminder, the goods and services traded on in cyber-security markets serve the primary purpose of establishing, preserving, and increasing the integrity and availability of information systems as well as the authenticity and confidentiality of their content. This encompasses the security of personal information.

As stated above, privacy products establish the promise of information control. This **implicitly includes the promise that the information systems and networks used in the transaction are also secure**. Such security is needed to uphold privacy provided by the final product.

[6] Jentzsch, N. (2007) Financial Privacy – An International Comparison of Credit Reporting Systems, (Springer Verlag, Heidelberg).

[7] The author thanks Volkmar Lotz for pointing this useful separation out.

## 2.2 KEY FEATURES FOR COMPARISON

After this clarification of concepts, we compare the key features of different products. Table 2 provides an introductory comparison of privacy and cyber-security with other types of goods, whether tradeable or non-tradable; traditional or "non-traditional."

The key features of economic goods are scarcity (and opportunity costs), excludability and rivalry, as well as indivisibility. Two additional features important for comparison are externalities and identity-association, the latter added by the author. All of these features will be explained in non-technical language in what follows.

Why are these features important? As such features determine the competitive strategies of firms, they merit an extra analysis. For example, if a firm produces information goods, it can version them. Versioning is not possible with apples.

Moreover, it is clear that **more and more products are becoming identity-related. The condition for such an association is the identification of the user.** Examples of identity-association include smart cars, smart homes, smart medicine, and electronic money; i.e. all services that allow personalization and tracking of the user.

If we assume that the characteristics of personal information (as product input) induce new competitive dynamics, we would observe them in more and more markets in future.

In the following, the key features for comparison are discussed.

**Theoretical scarcity** refers to resources that are limited, at least in theory. Much of economic theory is devoted to the efficient allocation of scarce resources and their 'best use'.[8] Apples, cars, gasoline and human kidneys are all scarce. Air is not seen as a scarce resource in economic textbooks.

**Practical scarcity** is introduced here as feature referring to the fact that once bound to a scarce medium or once polluted an abundant good can take on the characteristics of a scarce-resource good. Air can be polluted and therefore the amount of clean air is reduced. The number of CD-ROMs that can be produced

[8] Scarcity differs from depletion by way of definition. The latter describes the feature of resources provided by nature only once, with no chance of a future increase in quantity.

on earth is limited as well dues to the limited resources needed for producing them.

As the reader can see in Table 2, while information is theoretically not scarce (it can indefinitely be copied), it needs to be stored in a medium, like paper, digital media or the human brain, which implies practical scarcity.

**Table 2 Comparison of Traditional and Non-traditional Goods**

| Main feature | Traditional Goods | | | Non-tradable Goods | | Non-traditional Goods | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Apple | Car | Gasoline/ electricity | Air | Kidneys | Music CD | Cyber-security | Personal Data | Privacy |
| Theoretical scarcity | Yes | Yes | Yes | No | Yes | No | No | No | Yes |
| Practical scarcity[1] | Yes | Yes | Yes | Yes[2] | Yes | Yes | Yes | Yes | No |
| Opportunity cost | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes[5] |
| Excludable (use) | Yes | Yes | Yes | No | Yes | Yes | No | No | Yes |
| Rivalry | Yes | Yes | Yes | Yes | Yes | No | No | No | No |
| Indivisibility[3] | No | Yes | No | No | Yes | Yes[4] | Yes[4] | Yes[4] | Yes[4] |
| Identity-related[6] | No | No | No | No | Yes | No | No[7] | Yes | Yes |
| Externalities | No | Yes | Yes | No | No | No | Yes | Yes | Yes |

[1] Practical scarcity arises if the information is bound to a scarce medium (like paper).
[2] Practical scarcities arise when the resource is polluted.
[3] An indivisible good is a good that is sold in discrete quantities, like a car or a washing machine.
[4] A bit is an irreducible discrete unit of information.
[5] Privacy must be given up in order to achieve reciprocity or participation.
[6] Identity-relation refers to information about a person's identity that is not in the public domain.
[7] Correct is 'yes' and 'no.' As discussed above, there are products and services that can be identity-related.

**Opportunity costs** refer to the value of the second-best choice that is lost once given up for the first-best choice. If a car is used for driving to work, the opportunity of letting it sit in the driveway is lost. This feature does not exist in the same way with respect to information. As information can exist in several copies, it can be used for different purposes simultaneously, without foregoing the option of another, different and second-best use. For example, social graph information can be used to estimate a popularity score, but it can also be used simultaneously to estimate a credit score of a person.

Privacy, in general, has opportunity costs. Privacy (i.e. non-disclosure of personal information) must be given up in order to achieve something such as social reciprocity, access to a technology or participation in a network.

**Excludability and rivalry** are qualities, which are well-known in economics. The inverses (*non-excludability* and *non-rivalry*) describe key features of public goods.[9] *Non-excludability* describes the situation where excluding others is almost impossible, such as excluding others from looking at a light-house for orientation is an example. The second explains that some goods are non-rival in consumption (newspaper), while other goods are like bread. Personal information is characterized by both non-excludability as well as non-rivalry.

For cyber-security, it depends. For example, tap-proof telecommunications equipment is hardware that is excludable in use and rival in consumption. Cyber-security information products are only rival in consumption as far as it relates to the storage media used for it.

**Indivisibility** is also very important. An indivisible good is a good that is sold in discrete (countable) quantities, like cars or CD players. Information bits are irreducible units of information and in this sense, information **can be regarded as indivisible good** that is sold in discrete units, that is in bits.

Indivisibility also exists at the level of meaning, when we speak about intelligence, i.e., the interpretation of information. Here, we also find units of information that might not be further disassembled as their meaning will disappear.[10]

The term **identity-related** is not among the traditional features to describe a good. It describes the key feature of a good or service containing information about an identifiable individual (the 'data subject'). Traditional products like apples, washing machines or cars do not contain such information. While they can contain signals about the characteristics of an individual, think of an expensive car, they do not contain identification related information. **Identity relation** is based upon personal identification. It establishes a *personal relationship* between the individual and the product or service in use.

**As noted above more and more goods will turn into identity-related products and services in future (see Box 1).**

Identity relation allows a firm to infer a signal about an unobservable variable of interest, such as willingness-to-pay, payment risk, or purchase inclination. The exact pricing or product tailoring influences the division of the economic rent from a transaction between transaction partners. The side that is better able to predict

[9] The term 'public good' in economics does not refer to something that is 'good for the public' or should be in the public domain, it refers to a good that has the aforementioned key features.

[10] An address is only an address if it contains the name of the person, street, house number, zip code and town. If an item sold as address would only contain the first name of the individual it refers to, it would not be an address.

the other side's unobservable characteristic will be able to predict better the other side's behavior and can act upon this information. That 'knowledgeable side' is therefore more likely to reap a larger share of the rent from the transaction.

**Identity-relation can produce cognitive dissonance** if the data-collecting firm's interpretation of the information is not aligned with the individual's self-identity. While an individual might think that she is a physically active person, a fitness tracker might tell her that she is actually a couch potato.

Identity-relation, once noticed by the data subject, introduces psychological effects that do not emerge in conditions of anonymity. This is so because identification allows social sorting and social comparisons; the interpretation referred to above. Experimental research shows that identification leads to social conformism and more pro-social behavior (Haley and Fessler 2005, Nettle et al. 2013).

Another question is whether it is a key feature of a product to involve **externalities** that are non-monetary external effects placed upon other market participants. Those who use cars pollute the environment for others. Those who disclose personal information on websites allow statistical inferences made upon individuals that seem to be similar to them. Likewise, personal profiles stored in databases allow conclusions about those who are not stored in the database. For example, a comprehensive database of negative credit information allows conclusions about those not stored in the database. Note that for the latter individuals, no information was actively collected.

This holds vice versa, if all good types have an incentive to show that they are good, and no mimicry is possible, bad types are automatically co-revealed.[11]

**These information externalities show that information disclosure affects utilities of other market participants in terms of increasing the social classification power of firms.**

In relation to cyber-security, externalities refer to the problem that the security of one participant depends on the actions of other market participants with whom an interconnection exists. This introduces a structure of inter-dependent risks (Kunreuther and Heal 2003), which is essentially not over-seeable, not by individuals, firms, or governments.

[11] See Hermalin and Katz (2006).

## 2.3 So Is There Anything Special?

We have compared traditional goods, like a car that provides mobility, with non-traditional goods that provide cybersecurity and privacy. Where a car is a scarce good, excludable in use, rival in consumption and indivisible, it is – as long as it is not connected to the Internet – not intrinsically identity-related.[12] Once connected, though, the car would not only reveal the driving patterns of the driver, but also the driver's lifestyle (where he/she lives and works). It would also allow the estimation of the unobservable variables as discussed above.

Cybersecurity and privacy goods, on the other hand, are information goods and, as such, theoretically not scarce. Moreover, they are non-excludable and non-rival, because information has the same features as public goods. They are also to a certain extent indivisible (but not always), and in the case of pseudonymity and personalization products they are also identity-related.

So there are noticeable differences between traditional and non-traditional goods with a major difference in the key features of excludability and rivalry. That said, it does not imply that we need new economic models, as these key features are already well-known.

For personalized products, the most striking difference lies in the **establishment of a relation with the identified individual,** which has implications for the asymmetric distribution between the data subject and the firm. For years we had banking ad insurance services which are connected to individuals due to Know-Your-Customer policies. However, in economic models, such personalization as well as the externalities on the demand side did not play a role.

Most insurance models assume that the individual seeking insurance privately holds information concerning his/her risk. But this information asymmetry could tilt in future. An insurance company will have much better tools to predict the risk associated with an individual than the individual him- or herself. Instead of presenting many different options, the customer might obtain only one personalized version of the product, which is a very good fit.

The combination of key features (public goods, externalities) also increases the likelihood of market failure for these goods. But this is not something new as it is rather well-known in economics.

[12] Yes, cars need to be registered in the name of the individual. However, registration is not an inherent product feature.

In the cybersecurity domain the technical complexity of the products leads to greater information asymmetries.[13] But from an economics point of view this matters less, as models with asymmetric information are a 'working horse' in the discipline. So we may conclude that for cybersecurity we can apply many of the known models. Examples include cyber-insurance models (Shetty et al. 2010), information sharing models (Gal-Or and Ghose 2005) and security investment models (Kunreuther and Heal 2003).

For privacy products it is, to a lesser extent, explored how the identity-relation 'changes' the actual economics or renders known theories as obsolete. For example, identity-relation could lead to the conclusion that once individuals are identified, economic trade-offs are more prone to being overruled by other considerations (such as concern about social comparisons, reputation, etc.). There is certainly a sensitivity point in each individual, where this switch takes place.

In terms of the psychology that enters the trade-off, behavioral economics has made great strides on introducing models that explain divergences from the rationality theorem. Examples are salience (DellaVigna 2006), inequity aversion (Fehr and Schmidt 1999), and the endowment effect (Kahneman, Knetsch, and Thaler 1999). Researchers in this field study systematically the impact of psychological factors on economic decisions.

The only area where a real difference to traditional goods and traditional theoretical models could arise is where individuals **do not make economic trade-offs at all**.[14] If individuals do not make a conscious decision about their privacy, economic trade-offs would not matter and the same would hold for the theories that assume such reasoning. Individuals would act upon intuition only.[15] Such actions might not result in an optimal decision in a given situation. This would also mean that consumers would not choose the cheapest or the most secure seller, but other criteria might emerge as basis of their choices.

Decision-making, after all, requires cognitive resources. These are even higher if decisions involve multiple and complex trade-offs about the good to be purchased and about the information disclosure involved.

Further, personal information disclosure is, in many instances, a **sunk cost**: once the information is given away, it cannot easily been withdrawn or erased. It is known in

[13] Whether information technologies also bring about a more asymmetric distribution of power (i.e., a small group of hackers can bring down a country) is a different question.

[14] A number of cognitive scientists argue that most of the decisions we make *are not based on active conscious reasoning* (see Williams 2011).

[15] Heuristics are also increasingly becoming part of economic modelling.

the information security business that it is almost impossible to obtain a proof of total destruction of information.

Information is immaterial and as such difficult (if not impossible) to control. If cyber-security and privacy products and services promise such a control, much depends on the beliefs of the buyer as to whether the supplier can fulfil that promise. These beliefs can quickly change with security breaches. The inability to control its own information has been demonstrated by the National Security Agency,[16] a U.S. secret service agency with access to funds and technical knowledge far greater than private-sector companies. If the NSA cannot control secret information, the question is who can?

While the industry works diligently to increase cyber-security and reduce privacy risks, it is a Sisyphus task.

# III. CONCLUSIONS

In this paper, the tricky question is asked whether privacy and cyber-security goods and services are 'special' compared to traditional goods and services. As 'special' we would denote anything that differs notably from traditional goods.

The comparison with different kinds of goods showed that privacy and cyber-security have in fact features that differentiate them from traditional goods, tradeable and non-tradable ones. However, most of these features are known in economics and they are integrated in economic modelling.

But there are some features that merit future exploration. The most important one is the increasing identity-relation of many products and services that were formerly not associated with an individual. The second is the potentially uncontrollable nature of information and the information externalities that exist to a greater extent compared to traditional products, in particular once associated with the identity of a user or customer.

We also note that intuitive decisions could play a far greater role when it comes to disclosure of their personal information than acknowledged in the past. This could have major implications for consumer choice as well as switching.

[16] Wired (2014). Edward Snowden – The Untold Story, http://www.wired.com/2014/08/edward-snowden/

There is much to do in improving our understanding of what implications these observations for competition in privacy and cyber-security markets as well as markets in general.

# List of References


DellaVigna S. (2009). Psychology and economics: Evidence from the field. Journal of Economic Literature 47: 315-372.

de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. (2013). Unique in the Crowd: The Privacy Bounds of Human Mobility, Nature srep. 3, 1376.

Fehr, E.; Schmidt, K.M. (1999). "A theory of fairness, competition, and cooperation". *The Quarterly Journal of Economics* 114 (3): 817–868

Gal-Or, E. and A. Ghose (2005). The Economic Incentives for Sharing Security Information, *Information Systems Research* 16(2): 186–208.

Haley, K.J., and Daniel M., T. Fessler (2005). Nobody's Watching? Subtle Cues Affect Generosity in an Anonymous Economic Game. Evolution of Human Behavior, 26(3): 245–56.

Hermalin, B. & M. Katz (2006). Privacy, property rights and efficiency: The economics of privacy as secrecy, *Quantitative Marketing and Economics* 4(3): 209-239.

Jentzsch, N. (2015). State-of-the-art of the Economics of Cyber-security and Privacy, IPACSO Report Deliverable D4.1, published on ipacso.eu

Kahneman, D., Knetsch, J.L., & Thaler, R.H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *The Journal of Economic Perspectives, 5*, 193-206.

Kunreuther, H. and G. Heal (2003). Interdependent Security, *Journal of Risk and Uncertainty* 26 (2-3): 231-249.

Nettle D., Z. Harper, A. Kidson, R. Stone, I.S. Penton-Voak (2012). The watching eyes effect in the Dictator Game: It's not how much you give, it's being seen to give something, *Evolution and Human Behavior* 34: 35-40.

Schechter, S.E. (2004). Computer Security Strength & Risk: A Quantitative Approach, *research.microsoft.com/pubs/192264/thesis.pdf*

Shetty, N., G. A. Schwartz, M. Felegyhazi, and J. Walrand (2010). Competitive cyber-insurance and internet security, in T. Moore, D. Pym, and C. Ioannidis, editors, Economics of Information Security and Privacy, pp. 229-247, Springer-Verlag

Shapiro, C. and H. Varian (1999). Information Rules – A Strategic Guide to the Network Economy, Harvard Business School Press.

Williams, R. (2011). Wired for Success - Brain science helps redefine decision-making, Sept 25, 2011, https://www.psychologytoday.com/blog/wired-success/201109/how-can-we-make-better-decisions