ANASTASOPOULOU D. KALLIOPI

Privacy decision-making in the Digital Era

Submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

in

Information and Communication Systems Engineering

University of the Aegean

September 2016

HERACLITUS II: Doctorate scholarship with the aim of increasing the labour force of researchers through doctoral research implementation
ΑΝΑΣΤΑΣΟΠΟΥΛΟΥ Δ. ΚΑΛΛΙΟΠΗ

ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ ΩΣ ΠΡΟΣ ΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΠΟΧΗ

Σε μερική εκπλήρωση των απαιτήσεων για την απόκτηση του Διδακτορικού Διπλώματος του Τμήματος Μηχανικών Πληροφορικών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου

Πανεπιστήμιο Αιγαίου
Σεπτέμβριος 2016
Acknowledgements

I would like to express my deep gratitude to my supervisor Dr Spyros Kokolakis for his tremendous support throughout my PhD. With his guidance, I had the opportunity to explore the exciting topic of privacy decision-making. I am also particularly grateful to my other supervisors Dr Gritzalis Stefanos and Dr Pseiridis Anastasia. Moreover, I want to thank all the researchers involved in the Laboratory of Information and Communication Systems Security at the Dept. of Information and Communication of the University of the Aegean for providing me a unique environment that not only promotes creativity but also offers enormous support.

I also wish to express my appreciation to Dr Theodore Tryfonas for accepting me to work with him during my PhD studies at the “Systems Center” of the University of Bristol in the UK, within the frame of Erasmus Mobility Grant.

Finally, I would like to thank my parents and my brother who always encouraged me to pursue new opportunities in my career. Without their support, I would not have had the courage to make this step.
Dedicated

To

My mother

A strong woman who taught me to believe in hard work and that so much could be done with little

My father

For supporting and encouraging me to believe in myself

My brother

For being my guardian during my educational career
Abstract

Human activities that involve the Internet lead to the disclosure of personal information, either directly, as in the case of posting photos, videos and personal thoughts on an online social network, or indirectly, as in the case of purchase preferences revealed by consumers in an internet shop. Modern systems that can store and process vast amounts of information provide boundless capabilities for using and misusing personal information. Thus, information privacy has become a prime issue of concern for users, technologists, entrepreneurs, researchers and governments.

People negotiate their information privacy when they interact with enterprises and government agencies via the Internet. In this context, all relevant stakeholders take privacy-related decisions. Individuals, either as consumers buying online products and services or citizens using e-government services, they face decisions about the use of online services, the disclosure of personal information, and the use of privacy enhancing technologies. Enterprises make decisions regarding their investments in policies and technologies for privacy protection. Governments also decide on privacy regulations, as well as on the development of e-government services that store and process citizens' personal information.

Motivated by the issues and challenges above, this doctoral thesis focuses on aspects of privacy decision-making in the digital era and uses a variety of research methods to address issues of individuals' privacy behaviour and issues of strategic privacy decision-making for online service providers and e-government service providers.

Based on the Cultural Theory of Risk we study citizens' intention to use e-Government services from the perspective of decision biases. In this context, we present the results of an empirical study regarding citizens' intention to use a new service offered by the Greek Ministry of Finance, the so-called “Tax Card”. Tax Card has been used to collect information about everyday purchases and aims to diminish tax avoidance. We have examined the strong influence of Cultural Bias on the formulation of intention to use and concluded that different cultural types of people should be addressed in various ways to achieve broad adoption of e-government services.

Based on Behavioral Game Theory we introduce models of strategic interactions between users and enterprises. In this context, we study several cases. We present the strategic interactions of cloud-based online storage providers with sensitive privacy stakeholders. Privacy-related interactions are conducted between service providers and end users when the latter place their personal data in the cloud system. In this study, we use a game-theoretic model to analyse stakeholders' interactions and show how their behaviour can increase or not system reliability and also, improve or not the quality of service in a cloud computing content.
We also present an analysis of privacy-related strategic choices of buyers and sellers in e-commerce transactions. E-commerce transactions, in addition to the exchange of goods and services for payment, often entail an indirect transaction, where personal data are exchanged for better services or lower prices. This research work analyses buyer’s and seller’s privacy-related strategic choices in e-commerce transactions through game theory. We demonstrate how game theory can explain why buyers mistrust internet privacy policies and ignore privacy enhancing technologies (e.g. P3P) and sellers hesitate to invest in data protection. We propose a model of buyer-seller interaction that regards privacy policies as the basis of an agreement between a buyer and a seller, where the seller declares to follow the provisions of the policy and the buyer is expected (though not obliged) to be honest in providing information.

Furthermore, we analyse the issue of trust in Cloud Services by using the case of consumer trust in Cloud Services and the role of Security Certification. As individuals and enterprises add more and more information in the cloud, security and privacy concerns are growing. Potential consumers of cloud services do not have direct access to or detailed information about the cloud service provider’s infrastructure and the security measures implemented. As a result, they are not able to estimate risk, and they have to rely on the Cloud Service Provider (CSP) claims. Thus, asymmetry in information available to CSPs and consumers is introduced. A way to resolve the issue of asymmetric information is to engage third-party assurance. The above study aims to examine how asymmetric information on the security system implemented by the CSP affects the strategic choices of CSPs and consumers. Moreover, we examine the role of security certification and how it may change the strategic choices of consumers and CSPs.
Περίληψη

Οι ανθρώπινες δραστηριότητες που πραγματοποιούνται στο διαδίκτυο οδηγούν στην αποκάλυψη προσωπικών πληροφοριών, είτε άμεσα στην περίπτωση που κάποιος χρήστης ανεβάζει μια φωτογραφία, βίντεο και προσωπικές σκέψεις σε ένα άμεσα συνδεδεμένο κοινωνικό δίκτυο, είτε έμμεσα όπως στην περίπτωση που οι αγοραστικές προτιμήσεις των καταναλωτών αποκαλύπτονται σε ένα ηλεκτρονικό κατάστημα. Τα σύγχρονα μέσα μπορούν να αποθηκεύουν και να επεξεργαστούν μεγάλο όγκο πληροφοριών παρέχουν απεριόριστες δυνατότητες θεμιτής ή αθέμιτης χρήσης της πληροφορίας. Έτσι, η Ιδιωτικότητα αποτελεί πρωταρχικό ζήτημα μείζονος σημασίας για χρήστες, τεχνολόγους, επιχειρηματίες, ερευνητές και κυβερνήσεις.

Η Ιδιωτικότητα αποτελεί θεμελιώδες δικαίωμα του ατόμου, παράλληλα ωστόσο καθίσταται αντικείμενο διαπραγμάτευσης όταν οι άνθρωποι αλληλοεπιδρούν με επιχειρήσεις και διευθύνσεις κρατικών υπηρεσιών μέσω διαδικτύου. Σε αυτό το πλαίσιο όλοι οι εμπλεκόμενοι παίρνουν αποφάσεις που σχετίζονται με την Ιδιωτικότητα ή πιο συγκεκριμένα με την προστασία αυτής. Τα άτομα είτε ως καταναλωτές που αγοράζουν προϊόντα και υπηρεσίες από κάποιο ηλεκτρονικό κατάστημα, είτε ως πολίτες που χρησιμοποιούν υπηρεσίες ηλεκτρονικής διακυβέρνησης, λαμβάνουν αποφάσεις που σχετίζονται με τη χρήση ηλεκτρονικών υπηρεσιών, με την αποκάλυψη προσωπικών πληροφοριών και με τη χρήση τεχνολογιών προστασίας της Ιδιωτικότητας. Οι επιχειρήσεις παίρνουν αποφάσεις που σχετίζονται με επενδύσεις σε τεχνολογίες και πολιτικές προστασίας της Ιδιωτικότητας. Οι κυβερνήσεις επίσης αποφασίζουν ως προς νομικό πλαίσιο προστασίας Ιδιωτικότητας καθώς επίσης και με την επίτευξη υπηρεσιών ηλεκτρονικής διακυβέρνησης που αποθηκεύουν και επεξεργάζονται προσωπικές πληροφορίες πολιτών.

Υποκινούμενοι από τα παραπάνω ζητήματα και προκλήσεις, αυτή η διδακτορική διατριβή εστιάζεται σε διαστάσεις της Ιδιωτικότητας ως προς τη λήψη αποφάσεων στην ψηφιακή εποχή και χρησιμοποιεί πλήθος ερευνητικών μεθόδων για να εκθέτει ζητήματα που σχετίζονται με την πρόθεση πολιτών να χρησιμοποιήσουν μια νέα ηλεκτρονική υπηρεσία που προσφέρεται από το Ελληνικό Υπουργείο Οικονομικών, αποκαλούμενη ως «φοροκάρτα». Η «φοροκάρτα» έχει...
χρησιμοποιηθεί για τη συλλογή πληροφοριών που σχετίζεται με καθημερινές συναλλαγές και
σκοπεύει να μειώσει τη φοροδιαφυγή.

Έχουμε εξετάσει τη δυναμική επιρροή των πολιτισμικών προκαταλήψεων στο σχηματισμό της
πρόθεσης χρήσης και οδηγήθηκαμε στο συμπέρασμα ότι οι διαφορετικοί πολιτισμικοί τύποι
ανθρώπων θα πρέπει να συνυπολογίζονται με διάφορους τρόπους, με σκοπό να επιτύχουν την
όσο το δυνατόν καλύτερη υιοθέτηση υπηρεσιών ηλεκτρονικής διακυβέρνησης από πολίτες.

Βασιζόμενη στη Συμπεριφοριστική Θεωρία Παιγνίων (Behavioral Game Theory) εισάγαμε
μοντέλα στρατηγικών αλληλεπιδράσεων ανάμεσα σε χρήστες και επιχειρήσεις. Στο πλαίσιο
αυτό μελετήσαμε τρεις περιπτώσεις. Παρουσίασαμε στρατηγικές αλληλεπιδράσεις παρόχων
ηλεκτρονικών υπηρεσιών αποθήκευσης δεδομένων σε υπολογιστικά νέφη με εμπλεκόμενους
χρήστες που ενδιαφέρονταν να προστατεύσουν την Ιδιωτικότητα τους κατά τη διάρκεια χρήσης
αυτών των υπηρεσιών.

Οι αλληλεπιδράσεις Ιδιωτικότητας διεξάγονται ανάμεσα σε παρόχους υπηρεσιών και
tελικούς χρήστες, όταν τα προσωπικά δεδομένα χρηστών τοποθετούνται σε περιβάλλον
υπολογιστικού νέφους. Σε αυτή τη μελέτη χρησιμοποιούμε ένα θεωρητικό μοντέλο θεωρίας
παιγνίων για να αναλύσουμε τις αλληλεπιδράσεις των εμπλεκόμενων στο πάγιο και
deίχνουμε πως οι συμπεριφορές μπορούν να αυξήσουν ή όχι την αξιοπιστία του συστήματος
και επίσης, να βελτιώσουν ή όχι την ποιότητα των υπηρεσιών σε ένα περιβάλλον
υπολογιστικού νέφους.

Επίσης, παρουσιάζουμε μια ανάλυση στρατηγικών επιλογών Ιδιωτικότητας αγοραστών και
πωλητών σε υπηρεσίες υπολογιστικού εμπορίου. Οι εμπορικές ηλεκτρονικές συναλλαγές
eπιπλέον της ανταλλαγής αγαθών και υπηρεσιών με πληρωμές, συχνά εμπεριέχουν έμμεσες
συναλλαγές, όπου τα προσωπικά δεδομένα ανταλλάσσονται με καλύτερες υπηρεσίες ή
χαμηλότερες τιμές. Αυτή η ερευνητική εργασία αναλύει τις στρατηγικές επιλογές ως προς την
Ιδιωτικότητα πωλητών και αγοραστών σε εμπορικές ηλεκτρονικές συναλλαγές μέσω της
θεωρίας των παιγνίων. Αποδεικνύουμε πως η θεωρία παιγνίων μπορεί να εξηγήσει γιατί οι
αγοραστές δεν εμπιστεύονται πολιτικές Ιδιωτικότητας στο διαδίκτυο, αγνοούν τεχνολογίες
προστασίας της Ιδιωτικότητας τους (πχ. P3P), ενώ παράλληλα οι πωλητές διστάζουν να
επενδύσουν στην προστασία δεδομένων. Παραθέτουμε ένα μοντέλο αλληλεπίδρασης
αγοραστή – πωλητή που θεωρεί τις πολιτικές Ιδιωτικότητας ως τη βάση συμφωνίας ανάμεσα
σε ένα πωλητή και έναν αγοραστή, όπου ο πωλητής δηλώνει ότι ακολουθεί τις όρους της
πολιτικής και ο αγοραστής αναμένεται (αν και δεν υποχρεώνεται) να είναι ειλικρινής ως προς
τις πληροφορίες που παρέχει.

Επιπλέον, αναλύουμε το ζήτημα εμπιστοσύνης σε υπηρεσίες υπολογιστικού νέφους και το
ρόλο των πιστοποιητικών ασφάλειας, χρησιμοποιώντας την περίπτωση όπου ο καταναλωτής
εμπιστεύεται υπηρεσίες υπολογιστικού νέφους. Καθώς όλο και περισσότερη πληροφορία

ατόμων και επιχειρήσεων τοποθετείται σε περιβάλλοντα υπολογιστικού νέφους, τα ζητήματα ασφάλειας και ιδιωτικότητας αποκτούν μεγαλύτερη σημασία. Οι εν δυνάμει καταναλωτές υπηρεσιών υπολογιστικού νέφους δεν έχουν απευθείας πρόσβαση σε αυτό ή δεν έχουν λεπτομερή πληροφόρηση όσον αφορά την υποδομή ενός παρόχου υπηρεσιών υπολογιστικού νέφους και των μέτρων προστασίας που ενσωματώνονται σε αυτό. Ως εκ τούτου, δεν είναι σε θέση να εκτιμήσουν το ρίσκο και πρέπει να εμπιστευτούν τις διαβεβαιώσεις των παρόχων υπηρεσιών υπολογιστικού νέφους. Έτσι, η ασυμμετρία στη διαθέσιμη πληροφορία σε παρόχους και καταναλωτές εισάγεται ως έννοια στην έρευνα μας. Ένας τρόπος επίλυσης του θέματος της ασύμμετρης πληροφορίας είναι η εισαγωγή μιας τρίτης οντότητας που ελέγχει και πιστοποιεί την υποδομή του παρόχου. Σκοπός αυτής της μελέτης είναι να εξεταστεί πώς η ασύμμετρη πληροφορία επηρεάζει τις στρατηγικές επιλογές των παρόχων και των καταναλωτών. Επίσης, εξετάζουμε το ρόλο των πιστοποιητικών ασφαλείας και πως μπορούν να αλλάξουν τις στρατηγικές επιλογές των καταναλωτών και παρόχων.
List of figures
1-1 Describe the Information Flow................................................................. 15
2-1 Relationships between information privacy and other constructs (Smith et al., 2011) ...... 20
4-1: Overview of TAM ................................................................................. 47
4-2 Explaining “Social life” settings through grid/group dimensions........................ 50
5-1 The Buyer - Seller Privacy Game.......................................................... 70
5-2 Equilibria in variations of Buyer-Seller Privacy Game.............................. 72
5-3 The End-user -SP Privacy Game for Clouds.............................................. 81
5-4 Equilibria in Variations of the End user-SP Privacy Game in Clouds............. 82
5-5 Basic Model for CSP strategic choices for implementing ISMS................... 94
5-6 CSP – Consumer game with incident probability p ................................... 97
5-7 CSP – Consumer game with certification scheme, when security incident does not occur ......................................................................................................................... 99

List of tables
4-4-1 Items classified by Cultural Types........................................................ 53
4-2 The electronic Tax Card questionnaire...................................................... 55
4-4-3 Logistic regression analysis results......................................................... 57
4-4-4 Logistic regression results for the extended model with variables egal, fatal, hier, indiv, PEU, PPR, CI4 ............................................................................................................................ 59
5-1 Table 1: Present-value payoffs for repeated game ....................................... 98

List of equations
4-1 The regression coefficient of P ................................................................. 56
5-1 Equation for CSP with no incentive to deviate ........................................ 96
5-2 CSP decides to stop maintaining the ISMS............................................... 96
5-3 CSP with no incentive to deviate from the strategy ................................... 98
5-4 Present-value payoffs for repeated game................................................ 98
5-5 Bayes’ theorem: the probability for CSP to comply................................. 100
5-6 When CSP is compliant and applies for a certificate............................... 100
5-7 Consumer’s expected utility when CSP is certified.................................... 100
5-8 The expected utility by the probability that an incident does not happen...... 100
5-9 Consumer’s decision to buy from a certified CSP .................................... 100
5-10 Consumers benefit from purchasing and probability to lose from a security breach .... 100
5-11 If \( p \) is considerably small, then the consumer will buy.

5-12 CSPs best response 1

5-13 CSPs best response 2

Contents

Approved by the Examining Committee: ................................................................. 3
Advising Committee of this Doctoral Thesis: ......................................................... 3
Acknowledgements ................................................................................................. 4
Abstract .................................................................................................................. 6
Περίληψη .................................................................................................................. 8
List of figures ............................................................................................................. 11
List of tables ............................................................................................................. 11
List of equations ....................................................................................................... 11

1. Introduction .......................................................................................................... 15
   1.1. Information Privacy, Human Behavior and Privacy decision-making .......... 15
   1.2. Motivation, Research Questions and Objectives .......................................... 16
   1.3. Research Outline ............................................................................................. 18

2. Background and Methodology ............................................................................ 20
   2.1. Privacy decision-making: A Conceptual Framework ..................................... 20
       [2.1.1] Conceptual Map .................................................................................... 20
       [2.1.2] Values, Attitudes, Preferences and Choices .......................................... 21
       [2.1.3] Decision-Making Heuristics and Biases ................................................. 21
       [2.1.4] Information Privacy, Data Protection and Information Communication Technologies (ICT) ................................................................. 23
   2.2. Theoretical Foundation .................................................................................. 24
       [2.2.1] Online privacy concerns and privacy behaviour .................................... 24
       [2.2.2] Information Privacy and Data Protection: Standards and Regulations 26
       [2.2.3] Privacy decision-making: Biases and Heuristics .................................... 28
       [2.2.4] From Standard Economics to Behavioural Economics and Information Privacy ................................................................. 30
Standard game theory and Behavioral Game Theory: useful tools for decision-making under risk and uncertainty ................................. 33

2.3. Conclusions .............................................................................................................................................. 35

3. Literature Review ........................................................................................................................................ 36

3.1. Information privacy concerns, disclosure of personal information, and protective behaviours .................................................................................. 36

3.2. Privacy Decision-Making under the perspective of decision heuristics and biases 36

3.3. Self-Regulations, Firms and Governments Efforts in the Protecting Personal Information ........................................................................................................ 37

3.4. Privacy Economics ................................................................................................................................... 40

3.5. Privacy decision-making and its impact on e-government, e-commerce and cloud computing ......................................................................................................................... 41

4. Cultural Biases in the Information Privacy and Citizens Intention to adopt e-government services ......................................................................................................................... 44

4.1. Introduction and Theoretical Background ................................................................................................. 44

[4.1.1] A conceptual framework for e-government adoption factors .............................. 45

[4.1.2] Technology acceptance model (TAM) and related theories ............................. 46

[4.1.3] Perceived Privacy Risk ....................................................................................................................... 48

[4.1.4] Cultural Theory of Risk: Grid-Group Cultural Analysis ........................................ 49

4.2. Exploring Citizens’ Intention to use e-Government Services: The Role of Cultural Bias 51

[4.2.1] Overview of the Study ......................................................................................................................... 51

[4.2.2] Research Methodology ..................................................................................................................... 52

[4.2.3] Results and Analysis ......................................................................................................................... 57

4.3. Conclusions and Future Research ............................................................................................................. 59

5. Privacy-related Strategic Choices in Online Transactions: A Behavioral Game-Theoretic Analysis ........................................................................................................................................... 61

5.1. Privacy Tradeoffs in the Digital Age ........................................................................................................ 61

[5.1.1] Game theory fundamentals ................................................................................................................. 63

[5.1.2] Game Theory as a tool for decision-making ......................................................................................... 64

5.2. An Analysis of Privacy-related Strategic Choices of Buyers and Sellers in E-Commerce Transactions ...................................................................................................................................... 68
1. Introduction

1.1. Information Privacy, Human Behavior and Privacy decision-making

Information privacy is a multi-disciplinary and crucial topic for understanding the digital world (Regan, 2002; Acquisti, 2015). The information privacy usually refers to personal data stored on computer systems such as medical records, financial data, and business related information. Information privacy is synonymous with data privacy. In our research, the interest focuses on online privacy where all personal data shared over the Internet.

Current research on information privacy highlights issues referring to privacy attitudes and privacy behaviour. More specifically, privacy concerns of online users (Tsai et al., 2011; Acquisti et al., 2016) the privacy paradox between users’ concerns and their privacy-related behaviours (Young and Quan-Haase, 2013; Liang et al., 2016), and privacy-enhancing technologies (Parra-Arnau et al. 2014).

In the information age, privacy is thought as a luxury to maintain as data privacy can be breached in the internet world through cookies or tracking online activities (Pan and Zinkhan, 2006; Aguirre et al., 2016). The incredible growth of the internet and what it has brought to people’s lives especially during the past ten years is impressive. In the digital era, transactions are more convenient, and websites regarded as powerful communication channels where each information is available online.

Privacy, however, is not just an IT problem, although it could be in many cases. Many psychological, social and cultural factors play a significant role in privacy-related decisions. Human behaviour is a significant variable as individuals interact with others in online environments, exchanging private information and making decisions about their privacy. Privacy seems to be a central regulatory human process by which individuals make themselves more or less accessible to others.

Multiple factors affect the individual decision-making process regarded to the privacy framework. Bounded rationality, systematic psychological deviations and incomplete information, are referred in the bibliography as significant variables that influence the individual’s behaviour on privacy decisions (Acquisti, 2004; Adjerid et al., 2016). First, incomplete information appears when third parties share individuals’ private information.
without the others previously given permission. Incomplete information causes information asymmetries as individuals use their personal information, and take decisions, knowing possibly a subset of parties decision-making. The asymmetries create an imbalance in individuals’ decision-making, accompanied with uncertainties and risk to individuals’ data protection.

In the age of information, the asymmetries tend to be higher, the information more complicated, and all the above because of the acquisition and exploitation of the technology. Therefore, benefits and costs of data protection are also complex and multifaceted. For example, in case of a privacy incident, individuals search different things on internet and search engines send them the desired information. At the same time, search engines share individuals’ preferences to third parties. The above data intrusion has several extensions, some of which are directly measurable and some others not.

Second, with massive data produced every day, individuals are unable to control their data entirely and act optimally, even in case of having access to the complete information. In a complex world, counting consequences to disclosure of personal data seem to be impossible. Bounded rationality and heuristics prevent individuals from processing all relevant information without the clarity of mind. Very often, individuals adopt more simplified models and strategies, which are not adequate to depict a privacy incident in its actual dimensions.

Third, the literature identifies also systematic economics and psychological deviations that hamper individuals from taking a rational decision, even they have full access to complete information. For example, motivational limitations play a significant role in individuals decision-making. Also, experimental psychology shows that between losses and gains, losses weight heavier. Another interesting point is how prejudicially individuals estimate their future, because of wrong past decisions (Kahneman and Tversky, 2000, 2016).

Moreover, self-control problems often are responsible for individuals rational or irrational decisions. For example, during an e-commerce transaction, individuals usually disclose personal information to gain discounts or better services. Thus, they exchange their personal data with immediate gratification options. Additionally, social preferences and norms regarded as significant deviations to privacy-sensitive scenarios. Any of the above factors influence individuals decision-making decision behaviour directly. Empirical studies in economics and psychology insist that individuals not necessarily act against their actual concerns and needs. However, they indicate bias and limitations that privacy policy designers should consider carefully (Acquisti and Grossklags, 2005).

1.2. Motivation, Research Questions and Objectives

The central research objective is to explore and investigate the key challenges that influence individuals’ privacy decision-making in the digital era. Quantitative and qualitative
approaches adopted in the present research to investigate the drivers and inconsistencies of privacy decision-making and human behaviour.

Exploring the underlying reasoning behind people's privacy decision-making is a high motivation for our research. Motivation comes up from the following observation: Information privacy is negotiated when people interact with enterprises and government agencies via the Internet. All relevant stakeholders take privacy-related decisions. Individuals as consumers buying online products and services or as citizens using e-government services, face decisions about the use of online services, the disclosure of personal information, and the use of privacy enhancing technologies. Enterprises make decisions regarding their investments on policies and technologies for privacy protection. Governments also decide on privacy regulations, as well as on the development of e-government services that store and process citizens' personal information. Privacy decision-making from all the above parties discloses the privacy paradox phenomenon. The privacy paradox occurs when the marked contrast between privacy attitudes and actual disclosure behaviours. Also, the contrast between control over the publication, and control over the access and usage of personal information is at the centre of our research.

The above observation raises a few research questions:

a) How do people perceive and value their information privacy? This question aims to explore people's attitudes towards their privacy.

b) How do people value their information privacy in practice during the privacy trade-offs? This question focuses on people's actual disclosure decisions and how they evaluate the costs and the benefits of their decisions. The combination of the a) and b) research questions aim to investigate whether people's disclosure behaviours are paradoxical when compared to their privacy attitudes.

c) To what extent do people act as agents and to what extent are they influenced by specific structures during the privacy trade-offs? This question aims to uncover the extent to which people are constrained not to act entirely freely by specific structures.

d) Can we develop basic conceptual models of privacy decision-making that takes into account the dynamic nature of information privacy? This question was created based on the outcomes of the studies that addressed the previous research questions. The development of conceptual models that places the dynamic nature of privacy at the centre of its attention can offer valuable support to people's privacy decisions.

e) What are the key factors of the conceptual models? It is essential to identify the key factors based on the actual reasoning mechanisms behind people's privacy decisions.

In view of the foregoing discussion, our research has the following major objectives:
1. Present the feature of information privacy and explain why privacy decision-making process in the digital era under specific circumstances is so complicated.

2. Illustrate how conceptual models of Human Behavior with interests, beliefs, and intentions affect on Privacy decision-making.

3. Provide a critical examination of the existing literature related to privacy decision-making.

4. Analyze how privacy stakeholders behave when they have to trust, store and share their personal data into cloud-based environments and how a better understanding of their privacy decisions can be used as a tool for companies to create business value.

5. Explain why privacy decisions which involve risk and uncertainty have a significant behavioural economic impact.

6. Provide a coherent psychological framework underpinning the findings of the behavioural decision making.

7. We examine the strong influence of cultural bias on the formulation of citizens’ intention to use e-government services.

8. Indicate the way forward for the subject, regarding future challenges and areas meriting further research.

1.3. Research Outline

The structure and approach used in this doctoral thesis addresses the above research questions and serve our research objectives. In the first part, a conceptual framework analysis for privacy decision-making sheds light upon the various decision-making contextual elements such as values, attitudes, preferences and choices, decision-making heuristics and biases. Afterwards, a theoretical foundation analysis and our adopted research methodology around privacy decision-making highlight our research context.

Also, an extended literature review about: a) information privacy concerns, disclosure of personal information, and protective behaviors, b) privacy decision-making under the perspective of decision heuristics and biases, c) self-regulation, firms and governments efforts in the protecting personal information, d) privacy economics, e) privacy decision-making and its impact on e-government, e-commerce and cloud computing, map our research boundaries.

In the second part, we present the results of our research on privacy decision-making by developing conceptual models. Based on the cultural theory of risk we study citizens’ intention to use e-Government services from the perspective of decision biases. In this context, we present the results of an empirical study regarding citizens’ intention to use a new service offered by the Greek ministry of finance, the so-called “Tax Card”. Tax Card has been used to collect information about everyday purchases and aims to diminish tax avoidance. We have examined the strong influence of cultural bias on the formulation of intention to use and
concluded that different cultural types of people should be addressed in different ways to achieve broad adoption of e-government services.

Based on the behavioural game theory we introduce models of strategic interactions between users and enterprises. In this context we study several cases. We present the strategic interactions of cloud-based online storage providers with privacy sensitive stakeholders. Privacy-related interactions are conducted between service providers and end users when personal data stored in a cloud system. In this study, we use a game-theoretic model to analyse stakeholders’ interactions and show how their behaviour can increase or not system reliability and also, improve or not the quality of service in a cloud computing content.

We also, present an analysis of privacy related strategic choices of buyers and sellers in e-commerce transactions. E-commerce transactions, in addition to the exchange of goods and services for payment, often entail an indirect transaction, where personal data are exchanged for better services or lower prices. This research work analyses buyer’s and seller’s privacy-related strategic choices in e-commerce transactions through game theory. We demonstrate how game theory can explain why buyers mistrust internet privacy policies and ignore privacy enhancing technologies (e.g. P3P) and sellers hesitate to invest in data protection. We propose a model of buyer-seller interaction that regards privacy policies as the basis of an agreement between a buyer and a seller, where the seller declares to follow the provisions of the policy and the buyer is expected (though not obliged) to be honest in providing information.

Furthermore, we analyse the issue of trust in cloud services by using the case of consumer trust in cloud services and the role of security certification. As more and more information on individuals and enterprises is placed in the cloud, security and privacy concerns are growing. Potential consumers of cloud services do not have direct access to or detailed information about the cloud service provider’s infrastructure and the security measures implemented. As a result, they are not able to estimate risk, and they have to rely on the cloud service provider (CSP) claims. Thus, asymmetry in information available to CSPs and consumers is introduced. A way to resolve the issue of asymmetric information is to engage third-party assurance. This study aims to examine how asymmetric information on the security system implemented by the CSP affects the strategic choices of CSPs and consumers. Moreover, we examine the role of security certification and how it may change the strategic choices of consumers and CSPs.
2. Background and Methodology

2.1. Privacy decision-making: A Conceptual Framework

[2.1.1] Conceptual Map

In the digital age, concern about privacy issues is one of the major points of our times. We communicate primarily via emails, texts, and social media. Activities that were once private or shared with a limited number of recipients, now leave traces of data that expose our interests, beliefs, and intentions (Acquisti, 2015). Information privacy is of growing concern to multiple stakeholders including sellers, government regulators, and individual consumers. Privacy regarded privacy concerns as a measurable variable, because of the difficulty of measuring privacy itself. In social sciences, the majority of the empirical studies in privacy reckon on a privacy-related variable. Moreover, salient relationships are built more upon the perception than on rational evaluations (Smith et al., 2015).

In 1996, Smith et al. developed the concern for information privacy (CFIP) scale. They identified four data related dimensions of privacy concerns. These dimensions are the collection, the errors, the secondary use, and the unauthorised access to information.

![Conceptual Map](image)

2-1 Relationships between information privacy and other constructs (Smith et al., 2011)

Multiple factors prevent individuals from following the best decision-making process about their privacy. Incomplete information accompanied by bounded rationality and systematic psychological deviations are responsible for their decisions and an imperfect privacy-sensitive behaviour (Acquisti and Grossklags, 2005).
[2.1.2] Values, Attitudes, Preferences and Choices

Warren et al. (2011) insist that values, attitudes, preferences and choices be high-minded for decision making in the age of information. Individuals take decisions by thinking what is useful and desirable and what is not. Economists, psychologists and other behavioural scientists adopt the word “utility” to underline that the decision-making involves the clue of a subjective nature.

Behavioral decision scientists refer that we cannot measure values in a typical way. Utility theory measures values by checking individuals’ preferences. The decision which is preferable than the other is also the most valuable and demonstrate the expressed preference. Simonson (2008) refers that decision theorists equate preferences with choices or the willingness to pay or act. On the other hand, psychologists regard as preferences the consideration of what is desirable by an individual, and therefore interpret preferences to attitudes by scale rating measures (Gawronski and Bodenhausen, 2006). Attitudes are the tendency to respond positively or negatively to particular circumstances or individuals’ behaviours. Attitudes influences individuals to choose their action and chase challenges and rewards. However, we should underline that actual human behaviour is hugely different from the expressed attitudes.

Norberg et al. (2007) and Brandimarte, et al. (2013) transfer all the above knowledge to the field of privacy and data protection. More specifically, they consider that privacy perceptions differentiate between individuals and their actions. Researchers use various methods to evaluate individuals’ behaviours to privacy phenomena. Also, they focus more on privacy attitudes, intentions and concerns, rather than on their actual privacy behaviours and mechanisms that individuals adopt in their daily life.

[2.1.3] Decision-Making Heuristics and Biases

The most crucial question for individuals during a decision making is to recognise if their decision is right or not. Do they always follow an optimal decision strategy or not? An optimal decision is a decision that leads to the expected outcome. If there is uncertainty, then under the von Neumann–Morgenstern axioms the optimal decision maximises the expected utility (the utility over all possible outcomes of a decision) (Karni and Schmeidler, 2016).

Decision making is often a pretty-much complicated topic as it encloses behavioural constructs, cognitive and the psychophysical determinants. (Hagman, 2013). Many researchers work the last decades on cognitive heuristics and resulting biases as it is probably the best-known approach to explain how decision making is affected by all these human behavioural constraints (Gigerenzer, 1991 and Shiller, 2015).

The term “heuristic” is a Greek word and translated as “serving to indicate or to point out” (Gigerenzer and Gaissmaier, 2011). Several great mathematicians, economists, sociologists,
psychologists and other human behavioural scientists refer to this term in their research works. Einstein used the term “heuristic” in the title of his Nobel prize-winning paper in 1905 (Einstein, 1965). Max Weber is talking about the concept of ideal types and heuristics, suggests a three-step mechanism. Initially, he assumes that the individual act with full rationality, full knowledge, full awareness. Then, he matches the individual ideal behavioural with real actions, and at the end confront the ideal meaning with the empirical phenomenon and explain that the rationality of some social actions may vary under the circumstances and so may the knowledge and so on (Swedberg and Agevall, 2016). Much later, in 1970’s artificial intelligence (AI) researchers study how heuristics can solve problems, that logic and probability cannot. At the same period, psychologists use the term heuristic to explain why individuals take wrong decisions and how heuristics affect the human behaviour. Heuristics in 1970’s bind to biases and the gap in logic and probability theories, explained by the principles of sound thinking (Kahneman 2003, Tversky and Kahneman, 1974 & 2013). Gradually, theories around heuristics and biases influence the field of economics, behavioural economics and behavioural laws (Mousavi et al., 2016).

Heuristics are cognitive shortcuts, or rules of thumb, that allow people to act and decide with relative speed and accuracy. Individuals develop heuristics as they gain experience with a task, and heuristics improve (that is, become faster and more accurate) as a person’s expertise increases. Most heuristics are peculiar to a specific person, but some other heuristics such as availability, representativeness, and anchoring associate with a universal human behaviour (Tversky and Kahneman, 1974 & 2013).

Moreover, Payne et al. (1993) and Shah and Oppenheimer (2008) suggest that individuals search information to make the right decisions. The information search encloses a sort of trade-offs, where individuals rely on heuristics and biases to save effort, but with significant accuracy costs in some cases. More specific, individuals adopt a rational way of thinking as they believe that there are decisions which are essential, and others that are not. So, they choose shortcuts and save time and effort. Also, individuals during a decision-making face some cognitive biases which lead them to systematic deviations from standard rational behaviour, prevent them from acting rationally and force them to rely on heuristics.

Typically, a bias shows that the individuals ignore a part of the information in the base rate bias. They do not use the consensus information (the base rate) about how others behave in similar situations and prefer to adopt more straightforward ways of thinking which leads to arbitrary decisions with possible errors (Kahneman, 2003). Borrowing knowledge from the field of Staticians, Geman et al. (1992) suggest that there are three error sources: Error = bias + variance + ε, where “bias” is equal to systematic deviation which varies between the ideal model and the true state, “ε” is a clear random error.
In the digital era, more and more individuals use information and communication technologies (ICT) in their daily life. Future and emerging technologies create a significant impact on the whole society. However, the increasing use of ICT - either in the case of brain-computer interfaces, where computers are directly connected with human brains or in a simple case of an electronic transaction - involves fundamental rights challenges and arranges ethical issues. More specific, concerns about information privacy and the potential misuse of personal data in online environments is a reality.

Apart from examining ICT against current ethical issues, we have to consider that technological changes do not only influence information privacy by changing the way information is accessible, but also by changing the viewpoint with which we deal with privacy issues (Broenink et al., 2010 and Brey, 2012). For instance, individuals overshare personal information through social networks. Nowadays, the above behaviour is a common practice within certain groups. Such behaviours are expected in the era of emerging technologies and should be taken into account when trying to mitigate effects (Krishnamurthy and Wills, 2009).

Another crucial issue is whether hiding the information from parties is the appropriate method that we have to follow to protect our data from being misused. Janssen and Hoven (2015) and Gutwirth and De Hert (2008) suggest that data transparency and data protection are essential in the age of information. However, the only way to achieve transparency and protection over individuals information is by requiring data minimisation. That is, stakeholders should justify decisions over data about others and ensure that data collected and processed should not be further used unless this is an essential reason that supports data privacy. The above approach is fair enough but also, challenging. How should an individual prove that the decision he took was by using the wrong or the right information?

Transparency over data refers to the possibility of accessing information of others and how stakeholders behave during the disclosure process. Turilli and Floridi (2009) and Berkelaar (2014) argue that transparency is a pro-ethical condition to protect information, as both citizens and governments collect, store and process information about the others. This surveillance should increase the accountability as the choice to which information is or not accessible by the information provider may reveal the way stakeholders use the available information.
Emerging communication technologies have applications in many fields in today's digital world and can generate challenges to social effects and social sustainability. Technology-mediated interactions between an information sender and a receiver via a technology platform (e.g., an organization's website, cloud-computing platform) enclose dispositional, environmental and interpersonal privacy concerns. Dispositional privacy concerns exist when an individual has a concern about disclosing any information to other parties. Environmental privacy concerns caused by media reports, social privacy norms or family and friends beliefs. Interpersonal privacy concerns appear when an individual has privacy concerns about generally disclosing information about the party they transact with (Morton and Sasse, 2014). At that point and because the dissemination of information through technological means varies and can become ungoverned, a principle which can define actions in uncertain circumstances and ensure environmental privacy ethics is a necessity (Hilty and Aebischer, 2015; Pieters and van Cleeff, 2009; Som, Hilty and Köhler, 2009). This principle is known as the precautionary principle, and policymakers use it to justify decisions in uncertain environments where there is a possibility of harm when an individual has to decide, and the extensive scientific knowledge is lacking. Precaution could be used to impose restrictions at a regulatory level and contribute to the prevention of inappropriate information overloads from the users perspective. This protection measurement can be relaxed only in case scientists find sound scientific evidence that no harm will be caused to the decision maker and the public (Drexler and Fujimoto, 2015).

2.2. Theoretical Foundation

2.2.1. Online privacy concerns and privacy behaviour

In the age of information, information privacy (or data privacy) is extremely difficult to define, but also is the issue of our times. Privacy concerns apply in any place personally identifiable information is being collected, stored and processed. Acquisti et al. (2015) suggest that activities which are private or shared with others leave a trail of data that reveals interests, concerns, beliefs and interactions. Smith et al. (1996) recognise four different dimensions of individuals privacy concerns during their online transactions. These dimensions are the collection of personal information, the secondary use of personal information - without any permission from the original information source, any inaccuracy to personal information and the unlawful access to personal information (Dinev and Hart, 2006; Stewart and Segars, 2002).

In online transactions, the above concerns become more intense and focus on the control over data, possible misuse of personal data and standard practices that individuals have to follow to protect their data and their private life (Tucker, 2014). We recognise two basic actors: the first one is the consumer, the second one is the seller. The secondary unauthorised use of personal information - evoked by sellers, make consumers often to lose their trust (Camp,
Over the last decade, researchers study the conflict between consumers’ expressed behaviour on their data privacy and their willingness to sell information (Acquisti et al., 2015; Grossklags, and Acquisti, 2007; Wathieu and Friedman, 2007). It is shown that individuals as consumers may decide to trade-off their personal information if they want to earn benefits like better services, discounts or earn time during an online transaction((Acquisti et al., 2015; Aïmeur et al., 2016).

Moreover, the literature indicates that the individuals either as consumers or as citizens have privacy attitudes that very often differ from their actual behaviour (Acquisti et al., 2015; Smith et al., 2011; Tsai et al., 2011). The factors for the behaviour mentioned above include psychological deviations such as bounded rationality, cognitive biases such as information asymmetry or the sense of immediate gratification, irresponsible changes to individuals privacy sensitivities (Acquisti, 2004; Acquisti and Grossklags, 2005).

Information asymmetry plays a crucial role in decision making over data protection. Acquisti and Varian (2005) suggest that when the consumer buys something online, the seller try to collect much information about the consumer. Seller is interested in learning consumer’s identity, reservation prices, preferences and so on. By applying this strategy, the seller can group consumer preferences, create a profile for each consumer, make price discriminations, offer products and services that gratify the consumer immediately and increase his sales (Taylor, 2004; Acquisti and Grosslang, 2005; Acquisti et al., 2015).

The above information asymmetry exists when the one party (the seller) possesses greater knowledge than the other (the consumer) during an online economic transaction. Often, the consumer is not aware of how and in what extend seller use his data. The lack of such information, however, makes the consumer suspicious about seller’s intentions. Thus, the online purchase involves more uncertainty, and higher risk for consumers data as privacy policies are unknown. Therefore, the seller instead of increasing his sales, he managed the opposite results, as the consumer may be less willing to complete the transaction with a seller he does not trust. Nonetheless, another possible behaviour for the consumer is to engage in a risky transaction as he is unable to reveal the strategy that the seller follows. A privacy perspective for each party is very challenging in the online environments and looks like a game where stakeholders try to make optimal decisions, following dominant strategies and
gaining the highest benefit they can in each case and time (Acquisti and Grosslang, 2005; Nagurney, 2015).

[2.2.2] Information Privacy and Data Protection: Standards and Regulations

The internet is a globally interconnected network where computers and other electronic devices can be accessed promptly and anywhere. The open and dynamic nature of the internet empowers the dissemination of information through networks but also exposes internet users to specific information privacy vulnerabilities.

When individuals provide online information about themselves through online shopping transactions, social networking sites or otherwise, they expect this information to be protected. However, quite often networking technologies today place personal information at risk of unauthorised access or use.

Online privacy notices play a significant role in consumer privacy. An effective online privacy notice is an easy-to-follow guidance about how the information should be accessed, used, and protected. A comprehensive privacy statement is a standard mechanism for organisations to articulate various information practices and share them with the public. This statement covers issues such as the scope of notice, information uses and disclosures, choices available to end user, methods for accessing and processing personal information preferences and process for how any policies will be communicated to the public.

Individuals as consumers have the right to know if their information can be shared with another organisation or used for other purposes. The less information is processed by others, the more safety is provided for the online users. Limiting the second use of information is one of the fair information practices (FIPs). These practices are embodied in national laws, such as Privacy Act in the USA, EU Data Protection Directive and also international agreements such as the Organisation for Economic Co-operation and Development (OECD) Guidelines.

The EU Data Protection Directive emphasises the data subject’s fundamental right to access and correct personal information about the data subject. Article 10 states that the access and any correction should be provided where necessary to "guarantee fair processing in respect of the data subject" (EU Data Protection Directive, 1995). Subsequently, the General Data Protection (GDPR) adopted in April 2016 enforce and clarify some points on the Data Protection Directive with the goal to achieve data minimisation and limited process on personal information (Blackmer, 2016). In the United States, legal rights for individuals to access personal information held individually in sectors. For example, the Health Insurance and Accountability Act (HIPPA) of 1996 are medical privacy rules that protect personal health information and ensure health care access, portability and any preventive health care fraud and abuse (Benitez and Malin, 2010).
However, the Privacy Act of 1974 was a United States federal law that establishes a Code of Fair Information Practice (FIPs). The above federal practices are guidelines in the electronic commerce for the collection, maintenance, use and dissemination of personal data. Fair information practices recognise the individuals right to have the control over his data and know each time what information is collected or disclosed (Schwaig et al., 2006; Smith et al., 2011). The United States Federal Trade Commission’s Fair Information Practice Principles first refer to consumers’ right to have a notice of any party’s information practices before their personal data collected from them (notice/awareness). Second, in online environments, consumers should have the ability to control how their data used (choice/consent). Third, consumers should be able to have not only access to their personal data collected but also, the ability to verify the accuracy of data stored (access/participation). Fourth, parties who collect individuals’ data have to ensure that personal data they collect is accurate and secure (integrity/security). Fifth, organisations should ensure that they respect FIPs by adopting enforcement measures (e.g. self-regulation by the collectors or a regulatory body)(Belanger and Crossler, 2011; Gellman, 2016).

Additionally to the above practices and laws, we address four more internet privacy laws and standards to explain how organisations should behave on digital information about users and to what extent governments have access to citizens’ personal data. By providing all this information, we believe that we have covered the privacy law context for our research on privacy decision-making. The first law is the Electronic Communication Privacy Act (ECPA) which sets standards on how governments should have digital access information of citizens (e.g. emails, social media messages, cloud-based databases and other files) (Hernandez, 1988; Creech, 2013). Second, the Cyber Intelligence sharing and protection act (CISPA) is a federal law in the USA which indicates how organisations share information about cyber threats with the government (Backes et al., 2015). Third, the Computer Fraud and Abuse Act (CFAA) is a federal law which prohibits accessing a computer without authorisation or excess authorisation (Jensen, 2013). Fourth, the traffic – partnership agreement (TPP) is an international standard for online sharing information among nine countries along the Pacific Rim. The TPP arises issues for digital copyrights laws as both in the USA and internationally (Capling and Ravenhill, 2011).

Summarising, consumer access to information is an access-request problem for an unauthorised party. In case of a denial of access or correction request, the collectors should provide individuals with the reasons why and leave the individuals to challenge the denial. The principles around information security such as accountability, purpose specification, collection limitation, openness, data quality and individual participation, also extended to the web information environment. Thus, data protection and privacy professionals should consider which laws and policies apply to an individual request for access.
[2.2.3] Privacy decision-making: Biases and Heuristics

A full discussion of heuristics and biases is beyond the scope of our research. Early research works such as Bazerman and Moore (2009), Gigerenzer, et al. (1999), Kahneman (2011), Simon (1996), and Tversky and Kahneman (1974) focuses on how biases and heuristics influence the privacy decision-making process.

What actually are biases (or more correctly-given cognitive bias) and heuristics? Haselton et al. (2005) specify the term of “cognitive bias” as a systematic pattern of deviation from norm or rationality in judgment. In the early of the 19th century, the term of "heuristics" mentioned with a Greek origin (heuriskein) and referred to “enabling a person to discover or learn something for themselves”. Wherever an optimal solution is impossible, heuristic methods can be used to find a satisfactory solution. Heuristics assumed as mental shortcuts that help individuals to follow a cognitive path to make decisions and avoid the complexity of judgements. There are three types of heuristics: the representative heuristic, the availability heuristic, and the adjustment and anchoring heuristics (Tversky and Kahneman 1974). Representativeness means how much the “A” resembles the “B”. Availability refers to the ratio that a functional unit is capable of being used. Finally, anchoring is a term used in behavioural economics and present a cognitive error when we have for example to make an economic forecast. Adjustment and anchoring heuristic describes cases where individuals choose a goal or a value as a starting point, and then they adjust information until they reach an acceptable outcome.

A decision on information privacy involves subjective criteria and some uncertainty as individuals share their information in open-accessed and mobile environments. Tversky and Kahneman in 1974 suggest that “biases in judgements reveal some heuristics of thinking under uncertainty”. The first issue that we have to think is how decisions are made. Gigerenzer and Gaissmaier (2011) indicate three different directions: logic, statistics and heuristics. The approach of logic and statistics link to rational reasoning, while heuristics link to erring perceptions or irrational suggestions. Evans (2008) and Evans and Stanovich (2013) show that in the early 1970s, already in the psychological research Tversky and Kahneman (1974) introduces the heuristics and biases as two-systems reasoning. Later, Kahneman (2003) in his Nobel work attempts to obtain a map of bounded rationality. He explores the systematic biases that separate beliefs (the likelihood of an uncertain event) that people have, and the choices assumed in rational-agent models.

Heuristics do not result in optimal outcomes in any but the most straightforward problems. The errors that result from the application of heuristics are both random and systematic. Systematic errors (that is, systematic deviations from a normatively correct answer or
standard) are usually referred as biases. Discussions of biases in requirements determination specifically and systems development more generally (as well as other IS contexts) are available in Arnott (2006), Browne and Ramesh (2002), Stacy and McMillan (1995), West (2008), Ralph (2015) and Wickens (2015). Although all biases are cognitive, for research purposes, investigators have usefully divided biases into “cognitive” and “motivational” biases (Bazerman and Moore, 2009). Think the case where individuals buy services online, and the have to decide if they will sell personal information to gain some advantages. Two kinds of biases can affect individuals decisions. First, the cognitive biases are caused by how individuals process information (e.g., processes involving perception, and long-term memory). Second, motivational biases are caused by internal preferences or desires and by external forces and incentives in the decision-making environment.

So, why we need heuristics? Gigerenzer and Gaissmaier (2011) suggest that people save time, cost and effort with heuristics, but there is no accuracy on this method (Gigerenzer and Brighton, 2009; Reed, 2012; Klaube and Willekens, 2016). Heuristics trade-offs loss in accuracy as it is a faster solution with no need for high-level cognition. Thus, in rational trade-offs and because not every decision is important, people save time and effort by adopting shortcuts where the heuristics achieve a beneficial trade-off between the accuracy and effort/time. On the other hand, cognitive limitations prevent individuals from acting rationally and rely on a solution that may include judgmental errors for the decision-maker(Gigerenzer and Gaissmaier, 2011; Volz and Gigerenzer, 2012).

The last decades of research, biases and heuristics found to operate the individual's decision-making has changed, and they no longer fit into the three categories that Tversky and Kahneman discovered. Nowadays, cognitive scientists identify plenty of cognitive biases and heuristics in decision-making. Often, individuals adopt decisional shortcuts or heuristic strategies which may move to cognitive biases (systematic and predictable errors in judgment for now and the future). These biases result in the violation of rationality standards. More specific, the core standards of rationality are the principles of dominance and invariance and the sunk-cost principle. Dominance means that the individual will choose the option which is never the worse in comparison with the others. Invariance means that the information will be weighted and understood the same, regardless of how it will be presented. The sunk-cost principle means that because of the decisions influence the future; decision makers should weigh future consequences and not past behaviours or outcomes (Blumenthal-Barby and Krieger, 2015).

Summarising, we suggest that the most challenging direction is to find how biases and heuristics might be managed or countered when they are in fact harmful to privacy decision-making.
[2.2.4] From Standard Economics to Behavioural Economics and Information Privacy

All the economics focus on individuals behaviour in the sense of analysing how individuals allocate resources in different circumstances. Standard economics are very wide-ranging in their subjects area. Many ideas remain fundamental in economics and ignore all the behaviours studied by cognitive and social sciences. William et al. (1975) introduce a new theory where market prices differ from natural prices as the goods gain an added value, the value of exchange. Over the last decades, the standard neoclassical economic model based on the expected utility maximisation approach, suggest utility as a measure of individuals preferences over goods and services. The more utility they expect to have, the more they buy. In simple words, economists believe that utility reveals individuals willingness to pay different amounts for different goods (Dempsey, 2015).

The standard neoclassical economic model includes the following assumptions (Rumelt and Lamb, 1997; Dopfer and Potts, 2015):

- Individuals as economic agents are rational
- Expected utility maximisation motivates economic agents
- Selfish individuals concerns over the utility of others govern agent’s utility
- Agents are Bayesian probability agents (they interpret probability as a quantification of personal beliefs and not only as a propensity of some phenomena)
- Agents have time preferences according to discount utility
- All assets are completely exchangeable

However, a large number of empirical deviations appear as the standard economic model fails to explain. For example, why do sellers often value their goods and services much higher than buyers? Why is someone willing to see a ball game when he has paid for a ticket, but not when he has been given a ticket for free? Why do individuals decide to exchange personal information to have easy access to services or personal discounts? None of these questions is answerable by using standard economic models because the restriction nature of the standard economic assumptions involved and lead to inaccurate predictions.

Camerer et al. (2004) and Fudenberg (2006) suggest that questions such those mentioned above, need a more realistic psychological explanation and behavioural economics are suitable for that purpose, increasing at the same time the power of economics. Behavioral economics extend rational choices to equilibrium model and achieve more accurate predictions.

In our research, we focus on the economics and the information privacy. Privacy economics explain and measure the trade-offs according to the protection of personal information (Acquisti, 2010). The standard economic model of consumers behaviour over their personal
data is simple enough. As Varian (1996) explains that individuals as consumers buy the best thing they really can afford. In the last decades, many of the economics models accept rational and economically-sound individuals decision-making. Consumption bundles are the objects of consumers' choices. The description of when what and under what circumstances these goods and services would become available for the consumers is in the centre of standard economics interest. Any bundle can be described in the most simple terms as \((x_1, x_2)\) or just \(X\), where \(x_1\) denotes the number of goods and \(x_2\) the amount of another good, or amount of all other goods. By limiting the number of parameters to just two, it is possible to use an accurate graphical method of representation and analysis.

However, much of evidence from the field of experimental and behavioural economics shows that decision-making biases based on uncertainty and risk may influence the individuals' privacy behaviour. For example, online consumers may not adopt free-access privacy technologies to protect their data, as they probably do not trust their efficiency. The weakness of the standard economic model is already visible. Before discussing the weakness of the standard economic model, it is vital to clarify some terms that we will use extensively in this research work later on. The selected terms are “attitude”, “choice”, “value”, “preference”.

- **Attitude** defines as a psychological tendency to evaluate a particular entity with some degree of favour or disfavour (Chaiken and Eagly, 1996). A real characteristic of attitudes is that involve judgement, based on the concept of representation heuristic (Tversky and Kahneman, 1973, 1974). This kind of judgement leads to various kinds of extension bias such as the case where people recall past experiences to decide for their future. They ignore the length of an unpleasant experience, focusing more on the moment of the most intense pain.

- **Choice** is an action on the part of consumers, involving some decision-making. The standard economic model regards choices as merely revealed preferences.

- **Preference** is a level before making a choice. Economists assume that attitudes determine preferences.

- **Value** is a complicated term. It involves judgment. Psychologists and other behavioural scientists suggest that values determine attitudes. Economists, however, equals the term of value to the term of utility.

Wherever personal judgment takes place, predictions seem to be inaccurate. At this point, we can now consider the weakness of the standard economic model. The first problem relates to situations where the standard economic model makes inaccurate predictions and the second one relates to “silent” areas which there are no predictions and economists has no interest in these areas. This matter involves a subjective and restrictive value judgement regarding what economics should be concerned about.
Behavioural economics is a sub-field of economics which studies the effects of different behaviour factors from psychology and other behavioural sciences on individuals economic decisions. Behavioural economics studies the bounds of rationality of economic agents, and it integrates theories from psychology, neuroscience and microeconomic theory. It also includes market decisions, policies and mechanisms that drive public choice.

There are three major themes in behavioural economics: heuristics, framing and market inefficiencies. Heuristics shows that 95% of individuals make decisions using mental shortcuts. Framing refers to the way that stereotypes affect the individual’s emotional filters to understand entirely and respond objectively to events. Market inefficiencies include irrational decision-making on pricing policies (e.g., hyperbolic discounting) (Acquisti, 2004; Tsochou et al., 2015).

Behavioural economics is the link between a psychological approach to economics and neoclassical economics. Camerer (2002) and Frydman and Camerer (2016) refer that the field of behavioural decision-making has two basic categories: judgment and choice. Research on judgment is related to how individuals estimate probabilities, while choices are about how individuals select among actions, taking into their considerations judgment they have made.

The Carnegie Mellon University was one of the first research teams who focused their research on cognitive and behavioural biases, such as risk aversion behaviours for immediate gratification results. They are interested in finding if individuals have “irrational” behaviour about the decision-making and their privacy preferences. Systematic inconsistencies, and deviations, however, suggest the need for more productive theories to understand how challenges affect the way individuals make decisions for their personal information (Acquisti, 2004; Acquisti et al., 2015).

Acquisti et al. (2015) define the factors below as the main obstacles for rational decision-making over individuals privacy preferences. The framework of judgment; the conflicting needs (e.g., the need of publicity and the need to privacy); the incomplete information about risks and consequences over decisions for protecting personal information; the bounded rationality that restricts the individual’s ability to reflect on privacy-relevant actions have been identified as decision-making biases.

In online environments, individuals as consumers, make decisions about their personal data and their privacy. In the age of information, economics, behavioural economics, psychology, human-computer interactions and other behavioural and decision-making sciences focus their research on two principal directions. The first one is how to harmonise individuals need for privacy to their need for publicity (e.g., posting photos on social media - protecting at the same time their privacy). The second one is how individuals confront biases about privacy.
and security decision-making and how researchers can build better privacy technologies and information policies (Acquisti et al., 2016).

[2.2.5] Standard game theory and Behavioral Game Theory: useful tools for decision-making under risk and uncertainty

Game theory is relevant whenever there exists an interconnection in decision-making. In some cases, researchers focus their interests in games between firms and consumers involving pricing strategies and decision-making over consumers preferences. Game theory introduces some essential concepts: strategies, sequence, commitment and payoffs.

When the consumer “A” makes a decision (e.g., entry into a market), there would be a reaction of other consumers or firms to different strategies, usually regarding they act rationally, and interest of how these reactions will affect their utility. The other parties (called “players”) select their strategies, considering the reaction of the consumer (called “player”) A. In the above situation, each part decides risk and uncertainty (Fehr and Schmidt, 1999; Gintis, 2014). These situations apply in all areas of economics (e.g., bidding in financial economics, trade negotiation in international economics, oligopolistic pricing in microeconomics and so on). Game theorists come from different science paths, although mathematicians Neumann and Morgenstern (1944) and Nash (1951) regards as the pioneers of game theory.

The concept of a game includes three basic elements: players, strategies and payoffs. Players are decision-making entities whose utilities are interconnected. They would be individuals as consumers or citizens, firms, organisations, governments and so on. Strategies refer to a complete plan of actions for playing a game. It is vital to understand that in many games there may be many actions taken place. Payoffs are the changes in utility at the end of a game and determined as the choice of strategy selected by each player.

When players do not move simultaneously, and the sequence of the move is crucial, we should use the extensive-form representation of the game. Regarding different methods of analysis which are appropriate in different cases, we can classify game according to specific characteristics. Thus, there are cooperative and noncooperative games; two-player and multiplayer games; zero-sum and nonzero-sum games; perfect and imperfect information; static and dynamic game; discrete and continuous strategies; one-shot or repetitive games. To determine strategy or equilibria, we have to assume that players are rational utility maximisers. There are four appropriate strategies or equilibria in situations involving different payoffs: a) dominant strategy equilibria, b) iterated dominant strategy equilibrium, c) Nash equilibrium, d) subgame perfect Nash equilibrium, and e) mixed-strategy equilibrium (Wilkinson and Klaes, 2012).
The standard game theory involves three basic assumptions: a) players are motivated by self-interest, b) players have unbounded rationality and c) equilibria are reached instantly. The standard game theory is applicable in many situations where predictions are compared with empirical findings. Indeed, in games with mixed strategies predictions are accurate. In other cases such as bargaining games, its predictions may be inaccurate (e.g., uneven bargaining offers or rejected because of violating social norms of fairness). However, we often find that by relaxing the standard game theory assumptions and adding the appropriate parameters within the basic game-theoretic framework, we can improve predictions significantly (Camerer, 2011 and Wilkinson, 2008).

Thus, in our research work, we will be considering models that tend to use models that are somewhere between complex and standard models. More specific, we will examine two strands of analysis in behavioural game theory which are added to the standard game theory. The first has the basis of experimental evidence, where we examine many empirical studies to check anomalies arise from the standard model and the second come from the discipline of psychology, where behavioural game models have constraints not only from empirical evidence but also from psychology.

The second major area of research for behavioural economics after the behavioural decision-making is the behavioural game theory. Prior research on information privacy shows that individuals during an online transaction are eager to disclose personal information in exchange for some benefits. Empirical evidence from a game theory perspective ensures the above behaviour. A “privacy calculus” assessment on individuals personal information should be based on fairness on transactions, where consumers will share personal information, without unexpected results, such as the unauthorised second use of information (Culnan and Armstrong, 1999; Pavlou, 2003; Acquisti et al., 2015, Wallace, 2015).

Any interchange of individuals personal information can have positive and negative dimensions. Fehr and Gaechter (2000); Schram (2008) and Lumer (2010) suggest that individuals have a positive response regarding the fair interchange process, but also it can lead to sedative reactions under specific circumstances. Falk (2007), Kube and Puppe (2012) and Read (2016) report evidence from the experimental field due to individuals exchange behaviour. In collaboration with charitable organisations, researchers investigated the donation behaviour. Individuals who received a large gift with the donation letter invitation, are those decided to donate more. The behavioural game theory can model behaviours mentioned above by analysing the strategic movement of each player (e.g., individuals and charitable organisations).
2.3. Conclusions

This doctoral thesis focuses on aspects of privacy decision-making in the digital era and uses different research methods to address issues of individuals’ privacy behaviour and their strategic privacy decision-making. Individuals as consumers or citizens, online service providers and e-government service providers are the primary stakeholders in our research. Very often, individuals ignore what the other stakeholders (other individuals, organisations, governments) know about them or how stakeholders use that information. Most of the time, individuals decide what personal information to share online using their experience. They are familiar with evidence such as privacy breaches and the costs of the identity theft, but there are occasions where sharing a personal milestone online may drive to intangible costs. Also, the most policymakers underline that the control over personal data is a necessity to protect privacy. However, individuals tend to disclose more information if they feel that they transact in a trusted environment where low abuse on their personal data exists.
3. Literature Review

3.1. Information privacy concerns, disclosure of personal information, and protective behaviours

Researchers should identify the causes of privacy concerns to investigate the arising privacy issues in the digital world (Phelps et al., 2001; Smith et al., 2011). It is a fact that it is complicated enough to identify and measure privacy. Many important relationships are based more on perceptions and cognition, rather than on rational evaluations. Although in the field of social science beliefs, attitudes and perceptions are the leading representatives for privacy estimations, in the area of Information Systems (IS) conditions are different. There is a definite movement to privacy concerns. Variables such as “willingness to disclose personal information” or intention to make transactions are descendants of privacy concerns (Chellappa and Sin, 2005; Dinev and Hart, 2006; Buchanan et al., 2007). Hu et al. (2011) suggest that the institutional privacy assurances are responsible for explaining how individuals concerns can be shaped. In the field of IS, privacy concerns are concerns that reflect individuals fear of losing their privacy (Malhotra et al., 2004; Smith et al., 1996; Acquisti et al., 2016).

Margulis (2003) and Acquisti et al. (2015) refer that it is crucial to figure out general privacy concerns and situation-focused concerns. Bennett (1992), Solove (2008) and Sacharoff (2012) investigate the nature of privacy and argue that the concern around privacy is more understandable if we analyse use cases. Thus, in our research, we adopt the above recommendation and adjust the situation-specific context for privacy into consumer’s privacy concern when for example they visit a specific website and are dealt with the possibility of losing their privacy. The above worries stem from the fact that the individuals will decide to disclose some information to gain some beneficial services (e.g. extra discount on the next purchase).

3.2. Privacy Decision-Making under the perspective of decision heuristics and biases

Behavioural scientists are interested in investigating whether intentions, attitudes, or opinions can predict individuals’ behaviour over privacy. O’Keefe (2002), Norberg et al. (2007) and Brandimatre et al. (2013) note that individuals often behave in ways that differ enough from their declared intention. This phenomenon is called “privacy paradox” in the bibliography.
Although different approaches are referred in the literature from different research areas, all the researchers have similar observations about privacy concerns on the internet. All internet users confirm that they care about their privacy. However, they actually do so little to protect their privacy. The model intention-behaviour and how it really works is like the case with cars and seat belts. Drivers feel safe with seat belts in cars, but their driving habits (not wear seat belts very often) create an unacceptable level of risks for their life. Similar limitations exist when individuals manage their privacy in digital environments (Brandimatre et al., 2013).

Decisions for personal information are closely relative to costs and benefits of disclosure. Individuals should calculate costs and benefits to decide if they will reveal personal information during a transaction or not. In weighing the costs of disclosure, the decision maker should recognize risks under any decision for his personal information. A critical issue is the risk assessment, as risks are often unknown. Tversky and Kahneman (1974; 2013) talk about the “judgment under uncertainty”, where decision-makers rely on heuristics to make judgments under uncertain circumstances.

Decision-makers use heuristics as a tool to avoid complex calculations over probability and make a risk assessment. In cases where a rational approach is impossible, heuristics satisfies the decision makers need for an immediate decision, which very often drives to acceptable and positive results. However, in some cases, heuristics and biases are highly connected, and decision makers estimations are based on preferences and biases (Carey and Burkell, 2009). The heuristics-and-biases literature measures cognitive ability and thinking dispositions and connect the results with individuals will to adopt anchoring biases, preferences reversals, status quo biases, framing effects and so on (Toplak et al., 2011).

One of the most important reasons where decision-makers behave irrationally is related to a content problem. Namely, decision-making process is not only a procedural step but also involves analytical knowledge and strategic rules. Rational thinking errors may occur in large sets of knowledge bases in domains of probabilistic reasoning and logic thinking. Heuristics and biases derive from the idea of individuals as cognitive misers (Gilhooley and Fioratou, 2009; Toplak and Stanovich, 2014). Hoadley et al. (2010) refer that information privacy is based on the control over personal information and indicates that the perceived loss over control may be a function of objective reality and subjective beliefs, observations and biases.

### 3.3. Self-Regulations, Firms and Governments Efforts in the Protecting Personal Information

Self-regulation is highly connected with the sense of the control over information privacy. From the perspectives of individuals, firms and governments - perceived control over personal information creates interactions with different privacy assurance approaches such as
individual self-protection, industry self-regulation and government legislation (Hu et al., 2012).

Over the last decades, researchers are interested in investigating the concept of privacy concerns (Hu et al., 2012; Bansal et al., 2010, Angst and Agarwal, 2009; Dinev and Hart, 2006, Malhotra et al., 2004). Privacy concerns are strictly related to collection and use of personal information. Individuals adopt new technologies and make online transactions exchanging personal information. Hu et al. (2012) and Sun et al. (2015) suggest that individuals tend to have lower privacy concern if they believe that there is a certain degree of control over the collection and further use of their personal data. Thus, individuals tend to share more information effortlessly during their interactions. The above behaviour is advisable to examine it from a psychological perspective.

Culnan and Bies (2003), Son and Kim (2008), Smith et al. (2011) and Hu et al. (2011) ignore three critical approaches to the field of privacy protection: individual self-protection, industry self-regulation, and government legislation. These approaches focus on the individual control enhancing mechanism and the “agent” control mechanism. The first one is related to the individual’s self-protection and involves means where individuals directly control the flow of their personal information. The “agent” mechanism refers to government regulations and firms self-regulations where regulators or legislators act as control agents for the individuals’ data.

Therefore, stable government regulations and clear firms processes over individuals data processing are necessary to restrain any abuse of individuals personal information (Hu et al., 2012).

Prior research focuses on how the above approaches influence privacy beliefs and constructs such as perceived privacy risk, trust and privacy concerns (Son and Kim, 2008; Tang et al., 2008; Tang et al., 2015). Hu et al. (2012) and Bansal and Gefen (2015) analyse how interactions between firms, governments and individuals can influence privacy concerns through the perceived control mechanisms.

Firms self-regulations consists regulation privacy practices and codes of conduction (social norms, rules and responsibilities). In practice, third-parties provide trustworthiness to firms through their participation in associations such as Direct Marketing Association, or privacy seals such as TRUSTe. The above parties can confirm a high level of control over data and a sufficient privacy assurance level (Culnan and Bies, 2003; Bansal and Gefen, 2015; Kehr et al., 2015). A characteristic case of firms’ self-regulation is the TRUSTe case where privacy practices and implementation guidelines are prepared for local-based services (LBS) providers to protect private information (TRUSTe, 2004; Janson et al., 2014). Also, the Cellular
Telecommunications and Internet Association (CTIA) establish guidelines which protect from any abuse and illegal processing of personal data linked to location (CTIA, 2008). Therefore, firms adopting self-regulatory measures, avoid any opportunistic behaviour and at the same time, they increase their trust to individuals who need to interact on secure for their privacy environments. Hence, most of the online companies nowadays prefer to get certified with the TRUSTe privacy practices to approve that they care about individuals privacy and they are safe for any purchase or transaction (Wei et al., 2014).

From the firms perspective, empirical evidence has shown that third-party privacy seals can increase individuals control perception (Xu et al., 2012). Under government perspective, research has shown that privacy protection standards and regulations allow individuals to believe that government establish control mechanisms, and companies are obligated to comply with them. So, individuals feel safe and have the sense that firms will not disclose individuals personal information without their consent (Tang et al. 2008; Wei et al., 2014).

Having examined the “individual self-protection”, “firm self-regulation”, and “government legislation” approach, we can say that individuals weigh self-protection mechanisms and firm self-regulation as similar things. The above indication exists maybe because firms do not enforce enough their self-regulation or maybe individuals believe that they do not have an efficient way to react when firms misuse their personal information. Thus, individuals have to discrete carefully what information they share when they interact with firms.

The main point in this section remains the role of perceived control in “privacy concerns” frame. A psychological perspective of control is used with the control agency theory to examine the efficiency of three above mentioned privacy assurance approaches. The above interdependence is shown clearly in the literature where the three privacy assurance approaches link to with different types of control agencies. Metzger (2006) examines individuals privacy concerns to control mechanisms and recognise different types of control. The study with influences from theory-driven privacy interference shows that the more privacy assurance approaches do not necessarily drive to higher control perceptions. Also, the role of technologies is significant but remains a double-edged sword (National Research Council, 2007; Dinev et al., 2013). On the one hand, location-based technologies create many privacy challenges (e.g., data mining, and profiling), but on the other hand, privacy protections could be established through privacy enhancing technologies (PETs). Squicciarini et al. (2011) insist that IS researchers should examine PETS and integrate individual self-protection approaches in the IS privacy research.

Hu et al. (2012) suggest that with a high degree of self-regulation individuals may avoid the need for legislation, while with a high level of legislation cancels the need for self-regulation. Thus, the above three mentioned privacy insurance approaches influence the context-privacy
concerns of individuals. Concluding, future researchers and policymakers can view the above three mechanisms as a theoretical basis for developing a secure tool or practice guide for information privacy and a safer digital world.

3.4. Privacy Economics

Privacy economics are associated with costs and benefits around the protection or the possible disclosure of personal data. Data subject, data holder and the whole society are the primary stakeholders. Privacy economics as a research field is more active the last decades. Big data, data analytics, data mining are of high interest as they increase so the economic benefits, as the risks (Acquisti, 2013).

Advanced information technology development and any transmission to economics as a service, drive the organisation to collect store and analyse individuals data. All the above achievements raise significant privacy concerns (Acquisti, 2014). To investigate privacy from the perspective of economics, mainly when we focus on the field of big data we should adopt an economic assumption that belongs to the sphere of realisation. So, it would be rational to assume that all current privacy issues have monetary dimensions. However, data subjects and the decision-making over personal data are often a complicated situation. Any analysis of personal data is similar to welfare augmentation and economics inefficiencies reductions. At the same time, any processing on personal data is responsible for possible data loss or misuse, economic inequalities or a great concern of who actually controls data subjects personal data.

There are cases where an organisation prefers to use data mining technics to reduce inventory cost, but at the same time, data analysis conducted may arises privacy concerns. As a result, the organisation may lose its trustiness and achieve the exact opposite result. Also, a customer may prefer to know if other customers buy similar to his interest goods or services, but if they feel that they lose the control over the data, they may end up sharing personal information for price discrimination or other benefits.

Solove (2008) refers that the most dominant economic analysis over privacy focuses on the concealment of personal information. Akerlof (1970) with his work “the market for lemons” introduces the concept of information asymmetry. The seller may know how the consumer may behave before having any interaction with him (such as particular preferences for a good or service). After the purchase, the consumer may not know how the seller will use the information gained through a transaction. Stigler (1980) from the school of Chicago insist that the excessive protection of privacy may affect the quality of information which is available for sellers to decide their selling strategy. The above phenomenon can create various economic inefficiencies. Also, Posner (1981) argue that if an organisation have a little information about a candidate that is going to hire, it is possible to hire an unsuitable employee. Thus, the cost
is transferred from employees to employers, evoking economic inefficiencies and additional costs for the organisations. However, Hirshleifer (1980) and Taylor (2004) note that the neoclassical economics perspectives explain marketplace and stakeholders behaviour from a rational view. Logic may not capture the feature of a transaction as may involve risk and uncertainty over private information.

Some years later, Varian (1996) suggests that the dissemination of personal data is of high interest more for the organisations than the customers. However, it is noticeable that the same customer may decide to provide information in some cases (e.g., reserving prices for specific goods), while he may decide to conceal personal information in other circumstances. Noam (1996) notes that under free market exchanges, there is an equilibrium between the customer and the organisation - where the agent with the highest interest either to protect his data or robustly to access a database – will be the winner achieving its goal. However, there are two critical factors which influence individuals and organisations decisions over the most efficient outcomes for privacy and data protection. These factors are the uncertainty and the transaction costs.

In 2005, Acquisti and Varian worked on technologies which can track customers and identify them. They studied the economic impact of privacy and general prosperity. They suggest that rational decision-makers know that firms may track them and so they can change their decision strategy in a way to avoid any abuse of their personal information. So, firms should adopt a different strategy to have access to individuals data. They offer personalised services which are equal to the added value for firms and an excellent lure for individuals to disclose personal information.

In the age of information, privacy is a challenging topic as activities are shared, and trails of data reveal interests, beliefs and intentions (Acquisti et al., 2015). Firms and governments need to have access to personal data to offer better services and increased their profits. Privacy Economics explains the interactions between an individual as a customer or a citizen and the seller or the government over personal data from an economic point of view. The above interactions can be beneficial or costly for the stakeholders and the whole economy.

### 3.5 Privacy decision-making and its impact on e-government, e-commerce and cloud computing

E-government can alter the way government and customers (i.e. their citizens) were connected in the past. A new virtual government and citizen interface (Navarra and Cornford, 2005; Wong and Welch, 2004; Halachmi and Greiling, 2013) replaced the traditional approach. Silcock (2001) refers that the relationship between governments and citizens is a two-way relationship, creating a partnership relationship.
Literature highlights that the role of public administration and other government organisations, and their governance style, changing under the impact of, for example, globalisation (Bevir et al., 2003; Adams et al., 2014). The phenomenon mentioned above is also illustrated as the nature of public policy, both nationally and internationally, appears to be undergoing a significant critique and reconceptualisation (Ghose, 2005; Ghose and Pettygrove, 2015). These changes have implicated greater interest by governments to citizen attention as well as shifts towards forms of participatory governance. Lauber and Knuth (2000), Antony et al., (2004) strongly support the participation in the context of e-government. They believe that by involving citizens in decision-making for public topics (e.g., roads construction, new highways) is the right path to democratic governance. By incorporating citizens into policy designing processes, processes are more acceptable to citizens. The above strategic approach leads to a variety of benefits, ensures the implementation of management plans and improves the relationship between management agencies and the public administration (Irvin and Stansbury, 2004; Kim and Lee, 2012). Thus, e-government improves government accountability, making government more responsive to the needs and demands of individual citizens.

Apart from the impact on e-government, decision-making affects the e-commerce sector. In the era of electronic communication, privacy becomes an increasing concern (Berendt et al., 2005). Data are everywhere, and data sharing is a big issue at our times. Online users easily forget their privacy concerns to gain other benefits, such as easy access and they share even the most personal details without any significant reason (Berendt et al., 2005; Smith et al., 2011).

In e-commerce, online interaction between seller and buyers, the second often do not control his actions adequately. Buyers do not read privacy statements carefully on the web. They trust e-commerce environments even though they know that law and regulations do not always follow the rapid change of internet communications. Both stakeholders trust privacy enhancing mechanisms (PETs) as a better basis for their protection from cyber attacks or any tracking. P3P is an essential tool for privacy protection as if a website does not correspond to personal privacy preferences, automatic warnings appear. However, P3P is not adaptable to complex, intelligent infrastructure (Smith et al., 2011).

Research on the area of e-commerce and e-government refer to individuals intention to share information with sellers or e-government agents. Bélanger et al. (2011), Pavlou (2011) and Chellepa (2005) suggest that privacy concerns affect individuals intention to make online transactions. Individuals with higher privacy concerns, trust less and share less information (Dinev and Hart, 2006). However, Brown and Muchina (2004) and Tsai et al. (2011) argue that the unauthorised access to personal data by third parties - known as the secondary use of information - do not affect significantly users online privacy behaviour.
Belarger (2011) note that trust is more important than privacy when individuals decide to purchase online. Future research may prove why individuals intend to certain privacy practices to protect themselves from data breaches. Researchers suggest that there is a privacy paradox between individuals intention to reveal personal information and their actual behaviour ((Norberg et al. 2007, Berendt et al., 2005). Intentions lead to behaviours and actions. However, researchers should search more on information privacy and the impact on e-commerce and e-government environments, to explain why individuals often have a privacy paradox behaviour.
4. Cultural Biases in the Information Privacy and Citizens Intention to adopt e-government services

4.1. Introduction and Theoretical Background

The changing global digital environment increases competition among organisations (Tarhini et al., 2015) and supports new forms of interaction between governments and citizens. Government leaders continually invest in efficient e-government services for strategic reasons and organisational benefits (Casalino, 2014; Alenezi et al., 2015). From citizens’ perspective, e-Government is considered as a means to simplify procedures and streamline the approval process.

Access the various governments’ services at any time, and any place is undoubtedly a benefit for the above stakeholders. However, for citizens, the benefits of convenient services and easy access to information are often associated with risks of privacy violation and personal information misuse. As a result, governments often face resistance and limited acceptance of e-government initiatives.

Citizens’ willingness to share information is related to the spectrum of data, to those who will see it, and to the reason, the data are being collected (Olson et al., 2005). Several studies have shown that people do indeed value their privacy (Anton et al., 2010). Nevertheless, there are but a few studies that attempt to measure how much citizens value their privacy and the extent to which they differ in their valuations (Hann et al., 2002).

The effect of privacy risk perception on citizens’ adoption of e-government services is demonstrated as a key factor in the literature. Risk perception, in turn, is influenced by social and cultural factors (Douglas and Wildavsky, 1982). Douglas and Wildavsky (1982) have shown that cultural bias affects risk perception. Moreover, cultural bias affects people’s attitudes and choices in several aspects of their public life (see, e.g., Grendstad, 2000). It is, thus, expected that cultural bias may directly influence the adoption of e-government services.

For this purpose, we have surveyed Greek citizens’ intention to use the so-called “Tax Card”. Tax Card is an initiative launched by the Greek government in their effort to diminish tax avoidance. The Tax Card system is one of several e-government initiatives that were launched in the aftermath of the recent public debt crisis outbreak. The success of these initiatives has been considered crucial for overcoming the crisis. Initially, taxpayers were asked to collect receipts for their purchases and to present them to the tax authorities to qualify for the income-tax deduction. There were, however, serious complaints that receipt collection was a burdensome task and that paper receipts needed special care to be preserved until they are
delivered to the tax authorities. As a response, in October 2011 the Greek government issued the Tax Card initiative. The Tax Card records online taxpayer's purchases and enables tax authorities to monitor online retailers' turnover and the Value Added Tax (VAT) they should remit. Citizens would not need to collect receipts anymore and bring plastic bags full of receipts to the tax offices. However, the Finance Ministry had promoted the ambitious system of the Tax Card as a voluntary measure, and almost a year later, the system proved that it could not work. As of 2016 the measure is not formally abolished, but the majority of vendors do not have the Tax Card registration machines, and consumers do not adopt the Tax Card measure in their daily transactions.

Our aim, in the case above, is to determine whether cultural factors influence citizens' intention to use the Tax Card for transactions. This study took place when the government was still trying to convince people to use the Tax Card and has been based on a framework derived from both risk perception studies and approaches to cultural theory. However, we are primarily concerned with the following research question: To what extent cultural biases affect the intention of use?

In the following section, we present definitions of critical terms and the theoretical background of this research. Two relevant theories have influenced our work. The first is the Technology Acceptance Model (TAM), which is a well-studied construct with a long history of use in Information Systems (IS) research (Davis et al., 1989). TAM identifies the main factors that lead to the use of a new technology or system. The second is the Grid-Group Cultural Theory, which analyses the formulation of socio-cultural biases in people's behaviour. The second section includes an overview of the empirical study; the research methodology and the results of the empirical study. Finally, we present the main conclusions and topics that require further research.

[4.1.1] A conceptual framework for e-government adoption factors

While trust in e-commerce transactions is well established, factors that influence trust in e-government services need further analysis. Academic articles until 2015 show that the vast majority of published research has focused on the area of trust in e-government, emphasising to trust in government and to trust in the internet (Alzahrani, 2016). However, citizen's aspects of trust such as culture, education level, attitudes, beliefs, experience have not been sufficiently analysed.

The area of investigation brings in term-interpretations which are necessary to establish a common understanding of the used concepts. E-Government is the application of Information and Communication Technologies (ICT) which improves government's services, gains a competitive advantage over all stakeholders and transforms efficiency, effectiveness,
transparency and accountability to government and citizens (Almarabeh and AbuAli, 2010). Information Privacy is related with: (a) the collection of personal information, (b) unauthorised secondary use of personal information, (c) errors in personal information, and (d) non-authorized access to personal information (Smith, Milberg and Burke, 1996).

Perception of Privacy Protection: In the digital era where online services are of a highly interesting, privacy affects aspects such as the distribution or the non-authorized use of personal information (Wang, Norice, and Cranor, 2011). Bomil and Ingoo (2003) suggest that privacy protection ensures personal information about customers collected from their electronic transactions is protecting from disclosure without permission.

Culture (Uncertainty Avoidance): “The degree to which societies can tolerate uncertainty and ambiguity differ among cultures” (Hofstede, 1980). Uncertainty Avoidance: “The extent to which the members of a culture feel threatened by uncertain or unknown situations” (Hofstede, 2001). Cultural Bias involves a prejudice in an aspect that suggests a preference of one culture over another. Cultural bias can be described when there is a lack of group integration of social values, beliefs, and rules of conduct.

Privacy decision-making: The mechanisms that people employ when making online sharing decisions. Perceived Ease of Use (PEOU): The degree that users believe that using the system is easy or expects the target system to be free of effort and that it directly increases perceived usefulness (Davis, 1989; Rana et al., 2015).

Cultural Theory of Risk (or Risk culture): describes values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose. The above applies to all organisations from private companies, public bodies, governments to not-for-profits (Douglas and Wildavsky, 1982; Adams, 2016).

[4.1.2] Technology acceptance model (TAM) and related theories

TAM proposed by Bagozzi et al. (1992) as the most widely used innovation adoption model. This model has been used in a variety of studies to explore the factors affecting an individual’s use of new technology (Venkatesh and Davis, 2000). Davis (1989) suggests that “a key purpose of TAM is to provide a basis for tracing the impact of external factors on internal beliefs, attitudes and intentions”.

Even though TAM is a well-worn and familiar tool, it can still provide a new vision and value in each case. TAM is an advisable model that applies to many fields of research. It is an adjustment of the Theory of Reasoned Action (TRA) to the field of IS. TAM suggests that when users are presented with new technology, two factors influence their decision to use it or not. These factors are Perceived Usefulness and Perceived Ease of Use (see fig. 4-1).
Perceived usefulness refers to the effectiveness of the technology as perceived by a potential user. In other words, perceived usefulness is defined as the degree to which a person believes that using a particular system would enhance his or her performance (Davis et al., 1989). Perceived ease of use refers to the degree a person believes that using a particular system would be free from the effort (Davis et al., 1989).

| Perceived Usefulness | Behavioural Intention to use | Actual System Use |
|----------------------|-----------------------------|-------------------|
| Perceived Ease of Use|                             |                   |

4-1: Overview of TAM

Initially, TAM research was implemented in the framework of a settled and well-controlled group (i.e. employees), designing an information system that has been set by the company they worked for. Next generation researchers expanded this context to illustrate, for instance, e-commerce systems success. Davis’ work (1989) is used extensively in the IS literature to provide empirical evidence on the relationship between system use, usefulness and ease of use (Adams, et al., 1992; Davis, 1989; Hendrickson, et al., 1993; Segars and Grover, 1993; Subramanian, 1994). Attempts to extend TAM have taken one of three approaches: (a) by introducing factors from related models, (b) by introducing additional or alternative belief factors, and (c) by examining antecedents and moderators of perceived usefulness and perceived ease of use (Wixom and Todd, 2005).

On the other hand, there are related theories that deserve to be mentioned:

- **Theory of Planned Behavior** where adoption behaviour is preceded by behavioural intention which in itself is a function of the individual’s attitude, their beliefs about the extent to which they can control a particular behaviour and other external factors.
- **Social Cognitive Theory** is a framework for understanding, predicting and changing behaviour which introduces human behaviour as a result of the interaction between personal factors, behaviour and the environment.
- **Diffusion of Innovation Theory** as a social construct that gradually develops through the population over time.
- **Decomposed Theory of Planned Behavior** is an extended version of TAM, which models perceived ease of use and perceived usefulness as mediators of behavioural intention in which compatibility serves as an antecedent for both of them.
Unified Theory of User Acceptance of Technology notes that four fundamental constructs (performance expectancy, effort expectancy, social influence and facilitating conditions) are the primary determinants of consumers’ usage intention and behaviour.

[4.1.3] Perceived Privacy Risk

Perceived Privacy Risk focuses on "how people understand risk?" and "how the perception of risk influences decision making". Below we present ways where the term risk can be used. Also, we analyse the cultural theory of risk, psychometric paradigm and reviews several heuristics and biases that affect risk perception.

There are several formal descriptions of the term risk. We adopt the following: “Risk can be defined as the combination of the probability of an event and its consequences [...] In all types of undertaking, there is the potential for events and consequences that constitute opportunities for the benefit (upside) or threats to success (downside).” (IRM, 2002).

E-Government systems often face scepticism from worrying citizens that perceive e-government technology as a threat to their privacy. Perceived Privacy Risk (PPR) measures the degree to which a person considers a threat to his or her privacy as necessary. Risk can be considered as the product of the probability that an adverse event occurs and the associated expected loss. According to Featherman and Pavlou (2003), privacy risk is determined as the "potential loss of control over personal information, such as when information about you is used without your knowledge or permission".

Measuring risk is a challenging task even for experienced risk analysts. Therefore, we focus on how people perceive risk. Perceived risk theory was primarily applied in the marketing field with the aim to understand its effect on citizens’ purchase decisions under uncertain circumstances and with incomplete information available to them (Bauer, 1960). The field of Perceived Risk (PR) has been studied extensively over the last fifteen years. Many of these studies have recognised how much PR influences all levels of the buying process. Drawing from Perceived Risk Theory, Heijden et al. (2003) found out that PR is directly related to citizens’ online purchase behaviour. In this effort, they adopt a technology-oriented perspective and a trust-oriented perspective. Trust and risk, as far as perceived ease-of-use, and perceived usefulness was supported; while at the same time perceived risk and perceived ease-of-use result as predecessors of attitude towards online purchasing.

Moreover, each citizen’s intention to act is related to privacy concerns. Privacy is a problem with an economic feature, even when privacy matters seem too far from a direct economic
interpretation (Acquisti, 2004). Additionally, Acquisti (2013) refers that factors which influence individuals according to privacy decision-making are quoted below:

a) limited information about benefits and costs,

b) bounded rationality as an economic agent,

c) psychological parameters, such as self-control problems, underinsurance and hyperbolic discounting,

d) ideology and personal attitudes as factors that influence his/her privacy behaviour,

e) market behaviour such as propensity to risk, to gains or losses, and to bargaining.

Concluding, citizens mostly evaluate the likelihood of risk to their privacy, whenever they are engaged in a transaction (Cazier, 2008), and the result of this evaluation influences their intention to use the relevant technologies.

[4.1.4] Cultural Theory of Risk: Grid-Group Cultural Analysis

In this section, we discuss the different ways people understand and perceive different risks. The classical economic theories such as expected utility theory and the prospect theory suggest that all people try to act rationally, even though this rationality may be violated unknowingly.

The Cultural Theory proposes that many preferences that people make are due to culture the people choose to or are forced to live within (Wildavsky, 1987). Cultural Theory of risk is based on the work of Mary Douglas and Aaron Wildavsky. It was comprehensively described in their influential book Risk and Culture although the theory was based on their earlier work (Douglas and Wildavsky, 1982). The central claims of the theory are: everything people do is culturally biased, it is possible to distinguish a limited number of cultural types, and cultural types are universal (Mamadouh, 1999).

Further work on the theory includes several additional propositions: social relations and cultural bias must be mutually supportive (compatibility condition), there are only five possible culture types (impossibility theorem) and that each of the five culture types needs to be present in any society at any time (necessary variety condition). The culture types are resistant to change, and anything that does not fit expectations is explained away (theory of surprise).

The total number of possible cultures has been debated. Some academics see that there are only four types while others also include the fifth, autonomous type. This discussion is somewhat academic as the two dimensions, and four or five types is also mattered simplicity and usability of the theory (Bijker et al., 2012).
Cultural theory is based on a model introduced by Douglas and Wildavsky (1982) that distinguishes two central dimensions of sociality: grid and group (see fig. 1-2). A high grid way of life is strongly influenced by social structure and hierarchy, while a low grid one exhibits less respect for authority and social position. A high group way of life is characterised by social commitment and a high degree of social control, whereas a low group one emphasises on individual self-sufficiency.

The two axes of grid and group define four cultural types: egalitarian, individualistic, hierarchic, and fatalistic (Rippl, 2002).

| Grid | Group |
|------|-------|
| +    | -     |
| -    | +     |

**4-2 Explaining “Social life” settings through grid/group dimensions**

Citizens who belong to the category of egalitarianism are looking for active membership in groups, preferring to minimise external guidelines and rules. They are positioned at the low grid and high group quadrant. The fundamental values of this type can be expressed in one word: equality. The appropriate decision-making process for them is the consensus among the team members.

**Team spirit does not characterise individualists**, and they do not feel responsible for external requirements. They are positioned at the low group and low grid quadrant. They scorn strict rules and regulations, and they do not feel strongly the need to be bound to a group.

The fatalistic group consider themselves as subjects to external forces and that they believe they have little control over their lives. High grid and low group characterise them. The path of their life is more a matter of fate rather than personal choices. Equality is desirable, although it seems to be a utopia. This type of individuals experiences social isolation, such as the individualists, but they do not have the freedom of autonomy and the constraints of hierarchy. Also, they do not seek to join social groups.

Individuals in the category of Hierarchic tend to give priority to the welfare of the group where they belong, against their welfare. They are positioned at the high grid and high group
quadrant. They support the stratification of society and believe that social classes are defined and should be respected. They pay particular attention to social stability, norms and rules.

Cultural theory has influenced risk perception research (Dake, 1991). Several studies have shown that their cultural type biases people’s estimations of risk. Dake (1991) introduced a questionnaire for cultural type classification. Later, Rippl developed a new instrument and strategies to improve points of a scale that Dake had used in quantities studies in cultural theory and risk (Rippl, 2002).

The present work will focus on what can be stated as the relationship between the above four types of cultural biases and intention to use e-government services. The analysis is based on empirical data provided by an extensive survey of Greek citizens.

4.2. Exploring Citizens’ Intention to use e-Government Services: The Role of Cultural Bias

[4.2.1] Overview of the Study

Electronic government services have, in most cases, a two-fold objective: (a) to enhance citizens’ interaction with government and (b) to improve the effectiveness and efficiency of government operations. Thus, they are considered beneficial to both government and citizens.

Our first objective is to evaluate the effect of privacy risk perception on citizens’ adoption of e-government services. Risk perception, in turn, is influenced by social and cultural factors (Douglas and Wildavsky, 1982). Douglas and Wildavsky (1982) have shown that cultural bias affects risk perception. Moreover, cultural bias affects people’s attitudes and choices in several aspects of their public life (see, e.g., Grendstad, 2000). It is, thus, expected that cultural bias may directly influence the adoption of e-government services. Our second objective is to investigate the effect of cultural bias on citizens’ intention to use e-government services.

For this purpose, we have surveyed Greek citizens’ intention to use or not to use the so-called “Tax Card”. Tax card is a magnetic card the same size of a credit card. Bank branches deliver it to interested citizens, it is anonymous, and its use is voluntary. Afterwards, cardholders may send a short message to the Ministry of Finance with their Tax Registration Number and the number printed on the card. In this way, the card is associated with the taxpayer. Citizens may use several cards if they wish.

Tax Card is used at shops and enterprises that have Point of Sale (POS) terminals as they check out. The POS records the amount paid, date and time, the tax registration number of
the shop and the number of the Tax Card. This information is collected by the bank to which
the POS is connected and sent to the Ministry of Finance. It is there that purchase information
is associated with the citizen holding the card. At the end of the fiscal year, taxpayers receive
tax reduction benefits depending on their recorded purchases. The Tax Card project attracted
media attention and fears were expressed that citizens’ privacy was violated.

This initiative aims to address an essential issue of risk avoidance, as it was quite common for
shops and enterprises not to issue a receipt for most purchases, thus avoiding the associated
taxes. Before the Tax Card, citizens were collecting paper receipts, which were submitted to
tax authorities as an appendix to their tax declaration forms. However, there were many
complaints that citizens were devoting many hours to file the receipts and, also, they had to
keep them in a safe place, protected from moisture, heat, and sunlight, for about a year, until
they were submitted to tax authorities.

Tax Card was announced in 2010 but issued by the Greek Ministry of Finance in October 2011.
During the spring of 2011, we conducted a survey, which aimed to analyse the formulation of
intention of use. As probable factors, we identified (a) the perception of privacy risk, (b) the
cultural bias, (c) the perceived ease of use, and (d) the perceived usefulness. However, it
appeared that citizens that did not perceive the card useful (people with no or insufficient
income) had no intention to use the card and they excluded themselves from the survey,
which they considered irrelevant. Thus, we focused on the first three factors.

[4.2.2] Research Methodology

Instrument development

Rippl (2002) proposes a measurement instrument for cultural bias comprising eighteen items,
which can classify respondents in four types: (a) Hierarchists, (b) Egalitarians, (c)
Individualists, (d) Fatalists (see table 4-1). We adopted this instrument and translated the
items into Greek. Items were presented as bipolar questions. (Items CT1 to CT18, see table 4-
2.)

| Hierarchy | Egalitarianism | Individualism | Fatalism |
|-----------|----------------|---------------|----------|
| CT5       | CT4            | CT10          | CT5      |
| CT8       | CT1            | CT11          | CT7      |
| CT3       | CT6            | CT12          | CT8      |
Perceived privacy risk is measured by a single item (item PPR, see Table 4-2). A seven-point Likert scale was used. Similarly, Perceived Ease of Use (item PEU, see Appendix) was measured using a seven-point Likert scale. Finally, control items and demographics were included (CI1-CI4 and DG1-DG6, see Appendix).

Thus, a survey for the new electronic Tax Card was conducted and examined the risks of collecting personal data. The questionnaire used includes questions about citizens’ expectations and intentions to use the Tax Card, as well as questions relating to cultural and social perspectives. Responses kept confidentially and used only for this study.

| CT13 | CT9 | CT14 | CT2 |
|------|-----|------|-----|
|      |     |      |     |
| CT16 | CT11 | CT15 | CT10 |
|      |      |      |      |
| CT17 |      |      |      |
|      |      |      |      |
| CT18 |      |      |      |

4-4-1 Items classified by Cultural Types

Section 1 (Using Control Items to measure the impact of Risk Perception and Risk Attitudes)

**CI1**: Have you heard about the new electronic Tax Card?
(Yes /No/ Do not know-Do not answer)

**CI2**: Where did you learn about the card?
   a) Media
   b) Family environment and friends
   c) Your Accountant
   d) Others

**CI3**: Do you know what data will be collected through the card?
(Yes /No/ Do not know-Do not answer)

**DV1**: Do you plan to acquire it?
(Yes /No/ Do not know-Do not answer)

**DV2**: If not, why?
   a) It is in contrast with my moral values.
   b) I am afraid that the data collected by this system will be misused.
   c) I do not find it practical or useful.
   d) Other reason (please specify)

**CI4**: How much tax do you believe you could save by using the Tax Card?
a) Up to 100 € (income up to 10,000 €)
b) Between 100 € and 600 € (from 10,000 € to 20,000 € income)
c) Between 600 € and 900 € (from 20,000 € to 30,000 € income)
d) More than 900 € (30,000 € in revenue and over)
e) I cannot estimate

**PEU:** How much more consuming would you consider the manual collection and registration of purchase receipts? (Rating from 1 to 7, where 1 means very easy, and 7 means almost impossible).

**PPR:** How much do you fear that your data collected by the Tax Card system will be misused? (Rate on a scale of 1 to 7, where 1 means no and 7 mean too much.)

### Section 2 (Implementing Cultural Theory of Risk (Rippl, 2002))

- **CT1:** In family adults and children should have the same influence in decisions?
- **CT2:** There is no use in doing things for other people – you only get it in the neck in the long run.
- **CT3:** It is important to preserve our customs and cultural heritage.
- **CT4:** Important questions for our society should not be decided by experts but by the people.
- **CT5:** I would not participate in civil action groups. The ones in power do only allow what they like.
- **CT6:** It is important to me that in the case of significant decisions at my place of work everybody is asked.
- **CT7:** A person is better off if he or she does not trust anyone.
- **CT8:** We have to accept the limits of our life if we want or not.
- **CT9:** Firms and institutions should be organised in a way that everybody can influence important decisions.
- **CT10:** I do not join clubs of any kind.
- **CT11:** The freedom of the individual should not be limited for reasons for preventing crime.
- **CT12:** My ideal job would be an independent business.
- **CT13:** The police should have the right to listen to private phone calls when investigating crime.
- **CT14:** When I have problems I try to solve them on my own.
- **CT15:** I prefer tasks where I work something out on my own.
- **CT16:** Order is a probably unpopular but an important virtue.
**CT17:** I prefer clear instruction from my superiors about what to do.

**CT18:** An intact family is the basis of a functioning society.

### Section 3 (Demographics)

**DG1:** How old are you?

**DG2:** Male/Female

**DG3:** What is the level of education that you have already completed?
   a. Primary
   b. Secondary (High school)
   c. Tertiary (University/College degree)
   d. Master’s degree
   e. PhD

**DG4:** What is your profession?

**DG5:** What is your professional status today?
   a) Employee, b) unemployed, c) Inactive

**DG6:** Do you use Internet services and if so, how many hours a day around?

### 4-2 The electronic Tax Card questionnaire

#### Data collection

Data were collected through a national telephone survey, as a way to collect data systematically from a sample population, to maximise response rates and, also, to maintain control over the quality of the data. The telephone survey was based on a standardised questionnaire that combined knowledge from the socio-cultural field (Rippl, 2002), as well as from perceived privacy risk approaches.

A phone call was placed on 1152 citizens from all over Greece, to participate in research for the Greek Tax Card system. We had a positive response from 699 people, while 453 people refused to participate. The 529 of 699 citizens (namely 75.7%) have revealed their intention to use the Tax Card during their transactions and only 170 citizens (namely 24.3%) said they do not intend to acquire it. Also, all the 699 citizens answered to the related cultural questions.

Regarding the demographic profile of the Greek sample, we need to test and indicate whether the age, the educational level, the occupation and the use of the Internet services, affect or not the intention to use the Tax Card. The average age of 699 Greek citizens who have participated in the survey was 45 years. Doing the t-test, in this case, we find that the variable “age” is not statistically significant for their intention to get or not the Tax Card (see
As far as the variable “Education” (construct DG3) is concerned, we applied the Chi-Square method and found that the level of citizens’ education is a significant variable for their decision to use the Tax Card. Additionally, we applied the Chi-square method to find a strong correlation between “Employment” (construct DG5) and Intention to Use. Thus, citizens who are employed are more positive in adopting the Tax Card technology than the others.

**Model and Data Analysis**

With regard to Cultural Bias, we do not consider each individual belong to one category only. For each participant, we calculated his/her a score for each of the four categories. The score in each category is the sum of positive, relevant answers divided by the total number of valid answers. So, for each participant, we have four variables: Hier (Hierarchy), Egal (Egalitarianism), Indiv (Individualism), and Fatal (Fatalism).

Based on this questionnaire, we chose to implement regression analysis as it is applicable for modelling and analysing variables, especially when we want to find a relationship between a dependent variable and one or more independent variables. Regression analysis is used to find which among the independent variables are related to the dependent variable and show these relationships by a function of the independent variables, called the regression function. At that point, a large body of techniques for carrying out regression analysis exists. Nonlinear models for binary dependent variables include the probit and logit model. We have applied the logit model as it is the most prevalent in these cases.

In our model, P is the probability of Greek citizens to acquire the Tax Card. The formula can calculate the regression coefficient of P in our case:

$$P_{Tax Card INTU} = \frac{\exp (b_0 + b_1 * Egal + b_2 * Fatal + b_3 * Hier + b_4 * Indiv + b_5 * PEU + b_6 * PPR)}{1 + \exp (b_0 + b_1 * Egal + b_2 * Fatal + b_3 * Hier + b_4 * Indiv + b_5 * PEU + b_6 * PPR)}$$

The regression coefficient of P

Our model has as dependent variable the intention to use the Tax Card (Tax Card INTU) and as independent variables the four cultural types: Hierarchy (Hier), Egalitarianism (Egal), Individualism (Indiv), Fatalism (Fatal), and also the Perceived Ease of Use (PEU) and Perceived Privacy Risk (PPR) items from the Tax Card survey instrument (see Appendix).
Model validity

Before constructing the regression model, we had to examine if our model includes six independent variables (Egal/fatal/hier/indiv/PEU/PPR) or only the two ones (PEU/PPR). For this purpose, we have used the index "Akaike Information Criterion" (AIC). AIC is a measure of the relative goodness of fit of a statistical model. AIC provides a means for comparison among models and is calculated by the formula: \( AIC = 2k - 2\ln(L) \), where \( k \) is the number of parameters in the statistical model, and \( L \) is the maximised value of the likelihood function for the estimated model. The preferred model is the one which has the minimum AIC value.

In the first model, which has six independent variables, the AIC index has value 696.61. Likewise, in the second model, which includes two independent variables, the AIC index has value 699.61. Therefore, the best model in our case is the first one.

The results of the logistic regression on the six variable model are presented in the following table. Variables "HIER", "PEU" and "PPR" have \( P \)-value <0.05 (or 5%). That means that these variables are statistically significant.

| Variables | B   | S.E. | Sig. | Exp(B) |
|-----------|-----|------|------|--------|
| EGAL      | -.534 | .430 | .215 | .586   |
| FATAL     | -.650 | .406 | .110 | .522   |
| HIER      | 1.687 | .605 | .005 | 5.405  |
| INDIV     | .764  | .498 | .124 | 2.148  |
| PEU       | .109  | .056 | .054 | 1.115  |
| PPR       | -.257 | .048 | .000 | .773   |
| Constant  | -.178 | .675 | .792 | .837   |

4.4.3 Logistic regression analysis results

[4.2.3] Results and Analysis

Our survey has been answered by 699 persons. 247 respondents said that they intend to acquire the card, 284 said they are not going to get it, and 170 respondents were undecided. By running the logistic regression, we received the results shown in Table 2.
Coefficient B refers to the log-odds of citizens' intention to use the Tax Card, and S.E. refers to Standard Error. Also, the coefficient Ex(B) is the exponentiation of the B coefficient, which is the odds ratio. For example, the independent variable “Individualism” indicates that people who adhere to the individualist culture have 2.1 times more chances to form a positive intention of use. Finally, the Sig. shows the level of significance.

First, we notice the strong influence of cultural bias. The influence is strongest in the case of Hierarchists. We find that they are 5.4 times more likely to adopt the Tax Card and this result is statistically significant at significance level $a=0.05$. Hierarchists focus on social stability, procedures and rules. They respect authority and tend to trust the government. Thus, they are mostly willing to adopt government initiatives.

Second, we see that Individualists also show a strong tendency to adopt the Tax Card, while Egalitarians and Fatalists are less likely to use the card. Although these results are not statistically significant, they show a specific trend. Individualists will use the card if they find that they would benefit from its use. Fatalists are mostly indifferent, while egalitarians would object technology that gives the government more power over people, but they might adopt it if they believe that honest taxpayers would benefit from a more efficient public revenue system.

As expected, Perception of Privacy Risk has a negative influence on Tax Card adoption, while Perceived Ease of Use has a positive effect. However, it is shown that PEU does not have a strong effect. PPR has a stronger effect, but it is still far less influential than the cultural factors. Overall, cultural bias seems to be strongest, at least for specific cultural types, then privacy concerns and ease of use.

Finally, having processed and analysed data from several points of view, we should not neglect to examine the influence of the expected economic benefit of Tax Card users. The expected economic benefit is measured by item CI4, which refers to the number of tax citizens believe they could save by collecting receipts through the Tax Card service (see appendix). Respondents who replied that they could not estimate the amount they will save were excluded from the sample. Thus, the sample for this analysis was 200 respondents.

In this case, the independent variables are the egal, fatal, hier, indiv CI4, PEU, and PPR. Applying the logistic regression model the results are as follow:
### Variables in the Equation

|       | B    | S.E. | Sig. | Exp(B) |
|-------|------|------|------|--------|
| egal  | -3.976 | 1.274 | .002 | .019   |
| fatal | -3.481 | 1.088 | .001 | .031   |
| hier  | 1.884  | 1.239 | .128 | 6.581  |
| indiv | 2.084  | 1.201 | .083 | 8.035  |
| PEU   | .358  | .159 | .024 | 1.431  |
| PPR   | -.295 | .122 | .016 | .744   |
| CI4   | 1.019 | .332 | .002 | 2.771  |
| Constant | .743 | 2.049 | .717 | 2.102 |

4.4.4 Logistic regression results for the extended model with variables egal, fatal, hier, indiv, PEU, PPR, CI4

The above analysis shows that variables egal, fatal, PEU, PPR and the economic factor CI4 are very important for citizens who are going to decide about the use of Tax Card. People that expect a high economic benefit tend to adopt the Tax Card, as it would be expected.

### 4.3. Conclusions and Future Research

The effect of cultural bias is mostly neglected by policymakers. They focus on showing that e-government technologies are useful and easy to use and they attempt to downplay privacy concerns. These are important issues, especially the privacy issue. Nevertheless, often they fail to address the mindset of specific cultural groups that object these technologies. Egalitarians would not be easily persuaded that there are no risks to their privacy. However, they might set aside those concerns, if they come to believe that these new technologies would fight social inequalities and benefit a large group of people. Fatalists, on the other hand, are indifferent, in the sense that they would not make any effort to reach new technologies, but they would use it if they are “handed” to them.
E-government initiatives focus, to a great extent, on technology-related factors. We argue that e-government technology designers and policy-makers should also consider social and cultural factors. We believe that there is much to benefit from the social theory perspective.

In this research, we focused on intention to use. It would be most interesting for future research to examine the degree to which intention of use would lead to actual use. If not, it would be useful to study the factors that have deterred them from their initial perception. However, our analysis was limited to the Greek region and only to one specific e-government initiative, the Tax Card. It would be of high interest to conduct similar surveys to other worldwide cases.
5. Privacy-related Strategic Choices in Online Transactions: A Behavioral Game-Theoretic Analysis

5.1. Privacy Tradeoffs in the Digital Age

What are the privacy implications of behavioural decision-making in online transactions? To answer this question, we should notice what privacy stands for. For decades a long-lasting debate exists among scholars to define clearly what that right entails (Post, 1991). Undoubtedly, privacy is a fundamental human right (Warren & Brandeis, 1890), but also a “chameleon” that changes meaning depending on context (Kang, 2012). Looking for a privacy definition in the literature, we found clear disarray. Nobody seems to have a clear idea what the right to privacy is (Nofel et al., 2014). As Solove (2006) points out; privacy means different things to different people.

Warren and Brandeis (1890) described privacy as the protection of individuals space and their right to be left alone. Other authors have defined privacy as the control over personal information (Westin, 1970), or as an aspect of dignity, integrity and human freedom (Schoeman, 1992). Nonetheless, all approaches have something in common: a reference to the boundaries between private and public.

Privacy in the modern world has two dimensions. First, it has to do with the identity of a person and, second, it has to do with the way personal information is used. Individuals during their daily online transactions as consumers of products and services have many topics to consider and decisions to make related to privacy. Consumers seek maximum benefits and minimum cost for themselves. Firms, on the other hand, can take advantage of the ability to learn so much about their customers. Under the above prism scientists working on behavioural decision-making focus their research on the trade-offs and the protection (or sharing) of information (Acquisti, 2015).

Privacy transactions nowadays occur in three different types of markets (Acquisti, 2010). First, we have transactions for non-privacy goods where consumers often reveal personal information, which may be collected, analysed and processed some way. In this case, the potential secondary use of information considered as a possibility. The second type of privacy-related transactions occurs where firms provide consumers free products or services (e.g. search engines, online social networks, free cloud services). In these transactions, consumers provide directly personal information, although the exchange of services for personal data is not always visible. The third type of privacy-related transactions occurs in the market of privacy tools. For example, consumers may acquire a PET tool to protect their transactions or hide their browsing behaviour (Acquisti, 2013).

Consumers’ personal data analysis can improve firms’ marketing capabilities and increase revenues through targeted offers. Consequently, firms employ innovative strategies to allure
consumers to easily provide more personal information and shape preferences (Pitta, 2010). By observing consumers' behaviour, firms can learn how to improve their services and turn to price discriminations strategies for clear profit (Acquisti & Varian, 2005). On the other hand, consumers benefit from targeted advertisement strategies, since advertisements are tailored to consumers' interests. Firms and consumers can both benefit from such targeting; the former reduce communication cost with consumers, and the latter gain readily useful information (Tucker, 2011).

Finally, a more intangible but also surveyable form of indirect consumers' costs is related to the fact that the more an individual share data with other parties, the more those parties gain a bargaining advantage in future transactions with that individual. While consumers receive offers for products, data holders accumulate information about them over time and across platforms and transaction. This data permits the creation of a detailed dossier of the consumers' preferences and tastes, and the prediction of her future behaviour (Farrell, 2012).

Results from the literature on privacy transactions show that decision-making for the collection and diffusion of private information by firms and other third parties will almost always raise issues for private life. Consumers seem to act shortsightedly when they gain short-term benefits from trade-offs, even though there are long-term costs for privacy invasions. The behaviour mentioned above suggests that consumers may not always behave rationally when facing privacy trade-offs. Current research talks about the privacy paradox phenomenon where consumers face obstacles in making sensitive privacy decisions, as they have incomplete information and bounded access to the available information. Behavioural decision research suggests that consumers meet plenty deviations and behavioural biases during their daily transactions in electronic environments. (Acquisti, 2004; Acquisti & Grossklags, 2007).

Many scholars have argued trust as a necessity for successful e-commerce because consumers make purchases only if they trust sellers. Kim et al. (2008) introduce behavioural elements of trust in an e-commerce context, collect data from “successful” and “unsuccessful” cases, and provide a complete picture of business to customers decision-making process.

In chapter 5, we work on the game theory concepts suggesting them as a fundamental tool for decision-making under different circumstances. More specific, we present three different game theoretic models where players choose actions as sensitive privacy stakeholders that maximise their payoffs. They make optimal choices predicting the choices of the other stakeholders. First, we analyse privacy-related strategic choices of buyers and sellers in e-commerce transactions. Second, we present a strategic interaction analysis of the privacy-sensitive end-users use of cloud-based mobile applications. Our goal is to understand and analyse the low adoption of privacy policies in electronic environments. Third, we present a
strategic interaction analysis of the privacy-sensitive end-users who use cloud-based mobile applications.

[5.1.1] Game theory fundamentals

Briefly, we present core notions of game theory as an introduction to the following game theory concepts. Game theory suggests decision-making models under uncertainty where players choose actions that maximise their payoffs and looks for equilibrium by making optimal choices where each option is depending on the choices of other players.

Von Neumann and Morgenstern (1944) and Kuhn (2003) pose the game theory problem as following:

“If n players, P_1, ..., P_n, play a given game, how must the i^{th} player, P_i, play to achieve the most favourable result for himself? The elements of a game are:

- **Player** is the game participant; it can be an individual, company, nation, protocol, etc. There is a finite set of players P= \{1, 2 ... m\}.

- **Strategy** is the action taken by one player. Each player k in P has a particular strategy space containing a finite number of strategies, S_k= \{s_k^1, s_k^2, ..., s_k^n\}. Strategy space is S= S_1 \times S_2 \times ... S_m. The game outcome is a combination of strategies of m players: s= (s_1, s_2, ..., s_m), s_i \in S_i.

- **Payoff** is the utility received by a single player at the outcome of one game, which determines the player’s preference. For resource allocation, payoff stands for the amount of resource received, for example, u_i(s) represents the payoff of player i when the output of the game is s, s \in S. Payoff function U= \{u_1(S), u_2(S), ..., u_m(S)\} specifies for each player in the player set P”.

In literature, a significant number of game models are used to explain complicated decision-problems. In our work, we focus on cooperative and non-cooperative games. In game theory, a cooperative game is a game where players cooperate and make agreements (form a contract). The game regarded as a competition between coalitions of players. An exemplary case is a coordination game, where players choose the strategies by the majority of decision-makers (e.g. drivers choose the sides of the road upon which to drive). Niyato et al. (2011) study cooperative behaviour and cloud providers and refer that cloud providers join coalitions when the services offered to consumers incur an individual cost. In noncooperative games, players act with an objective criterion where each tries to make decisions that maximise his/her profit (e.g. two competing firms adopt similar pricing and advertising strategy to gain market share).

We also describe cases of imperfect, symmetric and asymmetric games. In imperfect information, players do not know the actions chosen by other players. However, they know
who the other players are, what their possible strategies/actions are, and the preferences/payoffs of these other players. The imperfect game assumes that when proposing their requests for cloud resources, all the users offer their bids at the same time and only know their bids/available resources. Symmetric games assume that all players have equal bargaining skills. In incomplete information sets (asymmetric games), players may or may not know some information about the other stakeholders, e.g. their “type”, their strategies, payoffs or their preferences. Concerning asymmetric games, users are competing for resources with different financial capacities.

Ardagna et al. (2011) refer to **Nash equilibrium** as “a set of strategies for the players constitute a Nash Equilibrium if no player can benefit by changing his/her strategy, while the other players keep their strategies unchanged or, in other words, every player is playing the best response to the strategy choices of his/her opponents. Therefore, a strategy profile \( \{s^*_1, s^*_2, \ldots, s^*_n\} \in S \) is Nash equilibrium if no unilateral variation in strategy by any single-player is gainful for that player, that is: \( \forall i, s_i \in S, s_i \neq s^*_i: U_i(s^*_i, s^*_{-i}) > U_i(s_i, s^*_{-i}) \).”

**[5.1.2] Game Theory as a tool for decision-making**

In standard economic models, individuals can think through problems and make choices unboundedly. Regardless the complexity of the problems, they manage to figure out optimal choices without significant cost. Individuals believe that every single problem has its solution and decide for each one. Every decision is perfectly calculated and quickly executed (Mullainathan and Thaler, 2001). A more modern approach to economics and other disciplines show that human rationality is bounded. Individuals often make decisions in a limited timeframe without having available full information. Decision-making in the real world often involves uncertainty and risk.

It is no surprise that the topic of decision-making under risk and uncertainty has fascinated observers of human behaviour from economists, psychologists to game theorists, strategists, management and behavioural scientists. **The risk** exists where the decision-maker knows with any certainty the mathematical probabilities of the possible results of choice alternatives. **Uncertainty** exists where the likelihood of different results cannot be expressed with any mathematical precision (Lee et al., 2016).

In chapter 5 a game theory approach is adopted as a very general language for modelling choices by agents in whom the actions of other agents can affect each player’s outcome. Each game has players, strategies, information, a specific game form (e.g. who chooses, when), outcomes (or payoffs - which are the result of all players’ strategic choices) and preferences over outcomes. The game theory language applies to many levels of analysis as it specifies analytical details of strategic interactions and matches to common categories of games such
as the prisoners’ dilemma game. The analytical game theory is the simplest form of a game theory language and refers to a game analysis where players have no previous experience in the game; that is “ideal” players with characteristics, which can be modelled easily. The analytical game theory assumes that players choose those strategies which maximise the utility of game outcomes, considering beliefs about what the other players will decide. Often, the most challenging question is how beliefs are formed (Bénabou and Tirole, 2016).

Most approaches suggest that beliefs derived from what other players are likely to do. In equilibrium, beliefs about others are equal to the question of how to specify reasonable beliefs by equating choices. However, some limits arise. First, many games that occur in social life are so complicated. At a particular time players cannot form certain beliefs of what other players would choose, and therefore they cannot choose equilibrium strategies. So, what strategies might be adopted by players with bounded rationality, or when there is learning from a repeated game? Second, in experimental studies, only received payoffs are easily measured such as prices in auctions. A huge variety of experiments shows that the analytical game theory sometimes explains behaviour adequately and sometimes is severely rejected by behavioural and process data (Camerer, 2003). The above inference can be used to create a more general theory which matches the standard approach when it is accurate and can explain the cases in which is severely rejected. This emerging approach is called “behavioural game theory” which uses the analytical game theory to explain observed violations by incorporating bounds on rationality.

The analytical game theory is the standard approach to analyse cases where individuals or firms interact, such as the strategic interaction of privacy-sensitive end-users use of cloud-based mobile apps or the e-commerce transactions between sellers and consumers. Behavioural game theory introduces psychological parameters which amplify a rational scenario and give a motivational basis for players’ behaviour. Representation, social preferences over outcomes, initial conditions and learning are the core components for a precise analysis (Camerer, 2003). However, in our work, we adopt a more generic approach using the analytical game theory language and present cases of strategic interactions through analytical game models.

More specific, we present three different game theoretic models where players choose actions as sensitive privacy stakeholders that maximise their payoffs. They make optimal choices predicting the choices of the other stakeholders.

In this chapter, we analyse three different game theoretic models, showing strategic interactions between sensitive privacy stakeholders who try to maximise their payoffs. Therefore, it is interested at this point to describe the environment where all these interactions take place, and present researchers work during the last decades on privacy games.
For this purpose, we focus initially on the information privacy and cyberspace transactions. Cyberspace is a terminology for the web of consumer electronics, computers, and communication networks that interconnect the world. The potential surveillance of electronic activities presents a significant threat to information privacy. Organizations collect and use consumers’ data, creating personalisation through privacy trade-offs, a strategic move that involves risk towards the protection of personal data.

The protection of privacy implements fair information practices which include a set of standards governing the collection and use of personal information. We use game theory to explore the motivation of firms to protect personal data and the impact to the social welfare in the context personalisation policies. Privacy protection can work as a competition-mitigating mechanism by generating asymmetry in the consumer segments of which firms offer customisation, enhancing the profit extraction abilities of the companies. In equilibrium, both symmetric and asymmetric choices of privacy protection by the businesses can happen, regarding how big are the personalisation scope and the investment cost of security. Moreover, as consumers become more concerned about their privacy, it is more likely that all firms adopt privacy protection. In the perspective of welfare, we show that free choices of privacy protection by personalising firms can increase welfare at the expense of consumer health (Lee et al., 2011). The regulations enforcing the implementation of fair information practices can be efficient from the social welfare perspective mainly by limiting the incentives of the firms to exploit the competition-mitigation effect.

E-commerce transactions, in addition to the exchange of goods and services for payment, often entail an indirect transaction, where personal data transferred to better services or lower prices. We analyse buyer’s and seller’s privacy-related strategic choices in e-commerce transactions through game theory. We demonstrate how game theory can explain why buyers mistrust internet privacy policies and relevant technologies (e.g. P3P), and sellers hesitate to invest in data protection.

Another reference and current research field related to privacy concerns in Cloud Computing. Free mobile applications of cloud computing offer a range of diverse services (such as gaming and storage) usually in return for delivering personalised advertising to their consenting end-users. Therefore, they may preserve personal data such as location and personal preferences. Thus, privacy-related interactions between service providers and end users are necessary to be studied as personal data are valuable in a subscription-based cloud system. In our research, a game theory approach used as a tool to identify and analyse such interactions to understand stakeholder choices, as well as how to improve the quality of the service offered in a cloud computing setting.

Game theory provides a robust analytical tool for the behavioural analysis of rational agents in many areas of social interaction, including privacy-related interaction. Researchers show
that rationality and the way it assessed play a central role in the analysis of human-computer interactions (Neth, 2016). However, assessments of rationality reflected on methods measuring it. Herbert Simon (1955 & 2016) suggests that human knowledge is bounded and adapted to its environment and ought to measured in it. Rational agents make decisions with limited information, assessed computational capacity, and in a specific timeframe. Constraints which occur during rational calculation considered the choices, the payoffs as a function of the option that is chosen, and the preference among payoffs. Choosing specific constraints, while at the same time rejecting some others in rational behaviour model leads to assumptions that control variables selected as a means of rational adaptation and other variables decided as fixed. For instance, different assumptions about the amount of information that the sellers and buyers have during an electronic transaction, concern the relations between alternatives and payoffs, optimisation might involve selection of a certain maximum, of expected value, or a minimax.

Rajbhandari and Snekkenes (2001 & 2010) introduce game theory to privacy risk analysis. They substitute probabilistic estimation of events and consequences with the results of a game theoretic analysis. They present the case of a user that subscribes to a service from an online bookstore. In this case, there are two players: the user and the online bookstore. The user can choose from two strategies, i.e. to provide accurate info or to provide false info. Bookstore’s plans include selling user’s information to a third party or protecting it. The mixed strategy Nash equilibrium gave the probabilities of each strategic choice and combined with the corresponding user’s (negative) pay-offs they provide a quantitative estimation of the level of privacy risk. By applying game theory, risk analysis can be based on preferences as a more subjective probability. Also, it can be used where no actual data are available. The above may increase the quality and applicability of the overall risk analysis process.

Friedman and Resnick (2001) analyse the use of pseudonyms as a game of M players (where M >1). In this model, users build online reputations based on pseudonyms and at each period they have the option to continue to play under their current identifiers or to get new ones. They show that this game is a repeated prisoner’s dilemma type of game and results in suboptimal equilibria. To avoid suboptimality, they suggest methods of limiting identity changes. Penna (2009) working on cost-sharing mechanisms and initiatives for pseudonyms suggest that incentives play a significant role in distributed systems. Typically, users want to get services from providers with the minimum information contribution. For example, BitTorrent is considered as a success since users can download data only if they upload some content to others. Such mechanisms rely on reputation are associated with the pseudonyms and probably are better.

Taylor et al. (2010) study the use of consumer data to exercise price discrimination. They analyse a model with a monopolist and a continuum of heterogeneous consumers, where
consumers can retain anonymity and avoid being identified as past customers, possibly at a cost. They conclude that when consumers can costlessly preserve their anonymity, they all choose to do so, which paradoxically results in a higher profit for the firm. Carbajal and Ely (2016) study monopoly price discrimination in cases where buyers care about consumption outcomes and their subjective beliefs. Acquisti (2013) suggests that by analysing massive amounts of consumer data, firms can predict trends such as variations in consumers demands that minimises inventory risks. Then, businesses offer useful recommendations to the consumer and enforce profit-enhancing price discrimination (Varian, 1985).

Otterloo (2005) studies the case of consumers that formulate their strategies because the shop is watching their strategic choices. Thus, consumer’s utility does not only depend on the value of the expected outcomes of strategic decisions but also on the information properties of the strategy chosen. They define two types of games, the minimal information game and the most typical game and show that in both games we can establish the existence of Nash equilibria.

Joshi et al. (2006) investigate the case of eBay-like auctions when a price-ascending auction is followed by a “second-chance offer”, i.e. a price-discrimination stage. They develop a game theoretical model and examine two possibilities (i.e. to provide or not privacy protection against anonymity and bid secrecy) and the corresponding privacy cost.

Concluding, current research has applied game theory in some specific privacy-related topics, and it has been shown that game theory can significantly contribute to our understanding of privacy-related behaviour.

5.2. An Analysis of Privacy-related Strategic Choices of Buyers and Sellers in E-Commerce Transactions

5.2.1 Overview of the study

E-commerce applications collect buyers’ data, either directly or indirectly. In some cases, buyers choose to refuse to deliver information about them, as in the case when they offer the opportunity to register and create an account at an electronic shop, which they may refuse if they believe their privacy is at risk. If an electronic store collects information indirectly, e.g. using recording buyers’ online behaviour, then buyers can use anonymity tools and techniques to conceal their identity.

On the other hand, electronic shops profit from personal data collection as they use them for reasons of marketing, pricing, and service improvement, or they only sell them to third parties, though this is illegal in many countries, in particular in the European Union.

In any case, information about customers is valuable for electronic commerce enterprises and, thus, they use various means to make customers reveal personal information. The latter
belong to two categories. First, there are incentives-based methods such as price cuts, participation in contests and prize draws, personalised services and recommendations. Second, there are trust-building techniques, such as privacy policies and privacy seals. An internet privacy policy is a statement that describes the ways a website gathers, uses, discloses and manages a rare visitor’s data. Although privacy policies are expected to promote trust in e-commerce, studies have shown that people read and hardly ever understand privacy policies (Cranor, 2003). Other studies have demonstrated that privacy policies tend to intensify privacy concerns instead of promoting trust (Pollach, 2007). Platform for Privacy Preferences (P3P) has been proposed to facilitate the use of online privacy policies. P3P is a protocol supported by the World Wide Web Consortium (W3C) that allows websites to state their intended use of the information they collect about site users in a machine-readable format (W3C, 2006). P3P enabled the development of privacy agents, e.g. Privacy Bird (Cranor et al., 2006) that can fetch P3P policies automatically, compare them with user’s preferences, and alert and advise the user.

Privacy agents have been proven to be usable and to influence web users (Vu et al., 2010). Nevertheless, neither P3P nor privacy agents have flourished. User adoption remains low (Beatty et al., 2007), and online privacy policies are, in most cases, ignored by standard users.

In this section, we follow a game theoretic approach in an attempt to understand and analyse the little adoption of P3P, privacy agents, and relative privacy enhancing technologies. We propose a model of buyer-seller interaction that regards privacy policies as an agreement basis for the buyer and the seller, where the second agrees to follow the provisions of the policy and the buyer is expected (though not obliged) to be honest in providing information.

Initially, we review the related work and present our primary model. Then we discuss the insights originating from our game theoretical model. Finally, the last part is devoted to conclusions and further research.

[5.2.2] The Basic Model

Consider an electronic shop that offers prices not significantly different from those of similar e-shops. This e-shop collects personal information to provide personalised services and publishes a well-structured (e.g. P3P-based) online privacy policy. A potential buyer examines the privacy policy and decides to proceed with a buy. Buyer and seller now have an agreement, though it might not be a legally binding one. The e-shop is expected to adhere to the declared privacy policy, and the buyer is supposed to provide valid information.

However, both have the option not to act as expected. The e-shop may sell customer information to a third party or use it in another profitable way that violates its privacy policy.
The buyer, on the other hand, may provide false information. In this way, the buyer gets protected from privacy violations but loses the benefits of personalised services.

Each player decides on a strategy based on his/her expectation of the other party’s behaviour. Thus, examining each individual’s behaviour separately would not allow us to understand the dynamics of the buyer-seller interaction. The above is a typical case where game theory constitutes an appropriate method of analysis.

The above buyer-seller interaction can be modeled as a game with both parties having two strategic options: to Cooperate (C) or to Defect (D). Cooperation for the seller means conforming to the privacy policy, while defecting means violating the policy. Respectively, cooperation for the buyer means to provide valid information, while defecting means faking personal information. So, there are four combinations (strategy profiles), which we present in the following paragraphs together with the corresponding payoffs.

If they both chose to defect, the buyer receives the minimum benefit, the one resulting from fulfilling the transaction. We arbitrary give it a value of one (1). Similarly the seller gets the minimum benefit arising out of selling the product, which we also give the value of one (1).

If the buyer defects, while the seller respects the privacy policy, then the buyer again gets the minimum benefit (1), and the seller will get the benefit of selling the product minus the cost of maintaining the privacy policy. Thus, we consider the payoff for the seller to be less than in the previous case, so we give it the value of zero (0).

If the buyer provides valid information and the seller mistreats it in some way, then the seller gets a significant profit, and the buyer suffers a loss, assuming that we have a privacy-sensitive buyer. We consider a payoff of three (3) for the seller and (0) for the buyer.

Finally, both of them cooperate, then they will both benefit. The buyer will get personalised services, and the seller may use buyer’s data, within the limits of the privacy policy. We consider a payoff of two (2) for each of the players. The game in standard form is presented in the following Table. Note that we use arbitrary values for the payoffs, for illustrative reasons. However, only the order of values is significant for the analysis that follows and not the exact values.

|          | Seller | Buyer |
|----------|--------|-------|
|          | C      | D     |
| **C**    | 2,2    | 0,1   |
| **D**    | 3,0    | 1,1   |

5-1 The Buyer - Seller Privacy Game
For the seller, defecting is a dominant strategy, since regardless of the buyer’s choice seller gets a better payoff. So, we can eliminate the dominated strategy for the seller (cooperate) and examine how the buyer would respond to the only remaining seller’s strategy (defect). In this case, the buyer will also defect. Thus, the equilibrium in the above game (often called the iterated dominant strategy equilibrium) is {Defect, Defect}. You may note that in the equilibrium state the overall payoffs are less than when both layers cooperate.

We have assumed that this game is played only once. However, a seller would normally expect the buyer to revisit the e-shop and make more transactions. So, if the game is repeated there are two more factors to take into consideration. First, whether there are finite or infinite repetitions and second whether seller’s policy violation gets detected. If policy violation does not get detected, then the iterative version of the game is identical to the one-off game presented above. So, we only examine the case of apparent policy violation, i.e. one that gets immediately detected, e.g. spamming.

In the finite case, the game is repeated several times and then stops. To find the solution for this game we should first examine the last round. We observe that the game played in the last round is identical to the one we presented above. Thus, the buyer would expect that the seller will violate the policy the last time the game it is played. However, for the buyer, it would be too late to fake its information. So, if the buyer assumes that at some time in the future the seller will mistreat the information provided, then he/she will fake its information from the beginning. Thus, the equilibrium of the finite repeated game is the same as in the case of the one-off game.

When a customer remains loyal to e-shops that consider reliable and makes regular buys, we may model the proper game as an infinitely repeated game, although it would eventually end at some time. The case of the infinitely-repeated game is more complicated. Since the buyer could stop buying from the particular e-shop (we do not consider monopolies), there is never an actual infinitely repeated game. However, we can simplify our analysis, if we examine the act of discontinuing the buyer-seller relation as a penalty imposed by the buyer to the unreliable seller. The penalty is equivalent to the loss of profit from all future purchases. While we leave the formal modelling and analysis of the game for future research, a rough analysis would show that respecting the privacy policy is a dominant strategy for the seller.

Concluding, the equilibria of the different variations of the buyer-seller privacy game are summarized in the following Table.
Results

Below we will try to interpret the results of the game theoretical analysis and discuss possible remedies. The previous analysis shows why it is hard to establish trust about the use of personal information in electronic commerce. Any e-shop that does not consider retaining its customers for an extended period to be a desirable or attainable aim would choose to exploit the personal information of its customers to maximise its profit.

Thus, in an internet market where customers move from shop to shop without any migration cost and without any benefit from remaining loyal to a particular e-shop privacy policies cannot establish trust. E-shops would not invest in developing and maintaining a strict privacy policy. Since consumers do not know in advance which e-shop is reliable and which is not, they will employ some privacy protection technique. In most cases, they would fake their personal information.

On the contrary, e-shops targeting consumers that would make regular buys and remain loyal if satisfied would refrain from mistreating personal information of their customers. However, this holds only for apparent policy violations. If privacy policy violations have a low probability to get detected, then the privacy-sensitive consumer would assume that the e-shop will mistreat his/her personal information and, thus, he/she will employ some method of privacy protection.

Thus, since voluntary privacy policies and relevant technologies, such as P3P and Privacy Agents, are not able to establish trust between sellers and buyers, we should seek for remedies. Our analysis shows that any solution should either address consumer loyalty or impose a penalty for violating sellers. Some options are:

- Regulate the use of policies by enforcing audits. However, one should consider the cost of audits and the possible low effectiveness, since such violations are notoriously difficult to detect.
- Impose high penalties for violating e-shops. However, this will only be effective if there is a reasonable detection rate.

|                        | One-off | Repeated | Infinitely repeated |
|------------------------|---------|----------|---------------------|
| Observable violation   | D, D    | D, D     | C, C                |
| Undetectable violation | D, D    | D, D     | D, D                |

5.2 Equilibria in variations of Buyer-Seller Privacy Game
By establishing reputation systems, an effective strategy in several cases is a fact. If privacy violating sellers expect to lose massively potential buyers, then they might not risk mistreating the personal information of their customers.

In any case, the above conclusions only apply to privacy-sensitive buyers. We should not disregard the fact that a large part of the population is not willing to put much effort in protecting their privacy, either because they feel that the information they reveal is not very sensitive, or because they feel that in the Internet world there is no practical way to protect your privacy.

This work has developed and analysed a game theoretical model to examine the inability of internet privacy policies to establish a trust relationship between sellers and buyers. It was shown that although it would be more profitable for sellers and buyers to be honest to each other and cooperate, the buyer-seller game will end in an equilibrium where the seller does not abide by the privacy policy and the buyer provides fake information. As a result, internet privacy policies are disregarded by consumers.

We have also shown that for privacy policies to have an impact on consumer they should be accompanied by regulations that impose a high penalty for violating sellers or reputation systems that increase the cost of violation.

Nevertheless, this study has several limitations as some potentially significant factors have been excluded. Specifically, we have excluded the consideration of discount of future benefits, which is a common factor in infinitely repeated games. We have only considered the game between a buyer and a seller, and we have not analysed the case of many buyers that communicate with each other and exchange information about the trustworthiness of sellers. Finally, we have not considered consumers that are not privacy sensitive.

5.3. Strategic Interaction Analysis of Privacy-sensitive end-users use of cloud-based mobile applications

[5.3.1] A brief introduction to Cloud computing and its key privacy concerns

Cloud computing is an excellent field of research, cited as 'the fifth utility' (Buyya et al., 2009), while at the same time considered as a useful tool for individuals, firms and other organisations. The interest in clouds concentrates on minimising fixed IT costs and using the IT resource with the maximum flexibility (Müller et al., 2015).

Various definitions of “cloud computing” exist depending on the usage scope. In our study we adopt the definition suggested by the US National Institute of Standards and Technology (NIST) where: “Cloud computing is a model for enabling convenient, on-demand network access
to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes the availability and is composed of five essential characteristics, three delivery models, and four deployment models.”

Cloud computing model as NIST proposes should consist of five essential characteristics:
a) **On-demand self-service** where a consumer can store his data without requiring human interaction with each server provider, b) **Broad network access** through standard mechanisms promote use by different platforms such as mobile phones, laptops, and PDA, c) **Resource pooling** where providers’ computing resources are pooled to serve multiple consumers demand by providing storage, processing, memory, network and virtual machines, d) **Rapid elasticity** where clouds capabilities can be provided and/or released, in some cases automatically, e) **Measured Service** where clouds automatically control and optimize resource use during storage and processing data (Mell & Grance, 2010).

As far as the relationship between the provider and the consumer concerned, four deployment models are introduced:
a. **Public cloud**, which is owned and operated by independent vendors and accessible to the general public.
b. **Private cloud** which is an internal technology, available to internal users within an organisation.
c. **Community cloud** is shared by several firms with common concerns such as security requirements, policy, and compliance considerations and may be managed by the firms or a third party. Healthcare community clouds or media clouds are typical examples.
d. **Hybrid cloud** which is a combination of two or more types of clouds (private, community, or public). An organisation may adopt private cloud for internal use, combined with public cloud technology to satisfy business needs (Mell and Grance, 2009).

**Cloud computing services** are classified into three layers:
a) **Infrastructure as a Service (IaaS)** which provides processing, storage and hardware resources practically via the Internet (Leavitt, 2009).
b) **Platform as a Service** which moves one step further than IaaS by creating applications using programming languages and joining a complete set of development tools, from the interface design, to process logic, to integration (Lawton, 2008a).
c) **Software as a Service (SaaS)** gives users mobile applications hosted as services. SaaS share with end-users the same code base maintained by the provider. Authentication and authorisation security policies are used to ensure the separation of user data. The cost and
price of SaaS sharing mechanisms (e.g. CRM or ERPs) allow them to stay competitive compared to traditional software. (Wang et al., 2011).

Yang and Tate (2012) report another classification framework in four categories:

a) **Technological Issues** which focuses on technology details of cloud computing (Cloud Performance, Data Management, Data Centre Management, Software Development, Service Management and Security).

b) **Business Issues** which refers to the business implications of cloud computing (Cost, Pricing, Legal Issues, Ethical Issues, Trust, Privacy and Adoption).

c) **Domains and Applications** which provide a general view of cloud computing practice and research (Foundational/Introductions and Predictions).

d) **Conceptualizing Cloud Computing** which discusses the impact of cloud computing on particular domains or applications (e-Science, e-Government, Education, Mobile Computing, Open Source and Other Domains).

In our research, we focus more on the business framework of Cloud Computing emphasising in the significant privacy concerns for privacy-sensitive end-users using cloud mobile apps. With cloud computing, privacy is an unavoidable concern when cloud users upload and store business or personal information (Katzan, 2010c). Cloud providers should shield the process and display clear policies about how user data is used (Ryan, 2011).

Privacy concerns are a mixture of security and confidentiality. Considerations involve the following domains:

**Access** where end-users should know what personal information is held and processed. The primary concern for organisations is the ability to provide individuals full access to all personal information and to comply with stated requests and regulations. However, can personal data be deleted by the organisation if they request for that? Moreover, if so, has it been removed in the clouds?

**Compliance:** What are privacy laws, regulations and standards which related to information stored in clouds, and who is responsible for maintaining the compliance?

**Storage:** Where data is stored? Some countries place limitations on the ability of organisations to transfer types of personal information to other nations. What happens in these cases?

**Retention:** How long personal information retained in clouds? Who enforces the retention policy and how is it managed?

**Destruction:** How does the cloud provider destroy (CSP) data at the end of the retention period? Did the cloud service provider destroy the data, or make it inaccessible to the end-user?
Audit and monitoring: How can organisations or end-users monitor their CSP and assure relevant stakeholders that privacy requirements are met in the cloud?

Privacy breaches: How do you ensure that the CSP notifies you when a violation occurs and who is finally responsible for that violation?

Privacy is a critical business issue, as it integrates social norms, human rights and legal mandates (Ackerman, 2001). Legal privacy requirements for organisations and consumers privacy expectations demonstrate the need for data control at all stages of processing, from collection to destruction. Cloud computing ability to scale rapidly, store data remotely and share services can be proved as a significant advantage, but at the same time, the difficulty in maintaining a sufficient level of privacy assurance and therefore confidentiality to potential customers is measured as a disadvantage.

[5.3.2] Overview of the Study

There exist many free cloud-based mobile applications (apps), which individuals can use to store their information into a cloud (e.g. Dropbox, Google Drive) or to access online services (navigation, gaming and so on). Users of these are usually faced with decisions that include a trade-off of handing over privacy-sensitive information (Brunette and Mogull, 2009). The term privacy-sensitive information refers to any personally identifiable information (e.g. name, address), sensitive information (e.g. religion or race, sexual orientation), usage data (recently visited websites) and also to unique device identities (e.g. IP addresses) (Pearson, 2009).

Services and applications that make use of privacy information into a cloud-computing context are components that can be implemented and scaled up or down, providing an on-demand utility model. Some of these applications include mobile social networking, real-time data processing and content delivery (Calheiros et al., 2009). Outsourcing data hosting functionality to the cloud through a secure platform-as-service is something increasingly utilised and offered at a low price (Brunette and Mogull, 2009). For example infrastructure services, platform and software applications are provided to end users of cloud computing through pay-as-you-go business models. Their more straightforward offering can take the form of free service in return for delivery of personalised advertising (that providers then make a profit from).

In this study, we follow a game-theoretic approach to understand and analyse how privacy agents behave when they have to trust, store and share their personal data into a cloud-based service (such as Google Drive) and how a better understanding of their privacy decisions can be used as a tool for companies to create business value. We propose a model where service providers and end users interact concerning general privacy policies for storing and sharing personal information. End users are expected to be honest in providing personal information.
to be subscribed in cloud services and on the other hand service providers are obligated to obey their privacy policies and do not disclose end users’ information to third parties.

We discuss related work in cloud computing, present and interpret our primary model. Then we present the initial results, which come out of this basic model. The last part contains our conclusions, and further research issues are addressed.

[5.3.3] Related Work

Data storage at a low cost, flexibility to pass services and better resiliency, are some of the benefits that give to end users a competitive advantage to adopt cloud-based services (Oscar and Andres, 2011). Individuals rely increasingly on cloud service providers to cover their computing needs; however, the pace of adoption of cloud technology is not excessively quick, as people and organisations do not migrate critical systems to cloud computing yet. The same happened in the past with technologies like virtualisation, where stakeholders started to use them for non-critical systems, and when they became comfortable with the new technology, they used it for all type of systems.

In the literature, the most studies of cloud computing adoption are conducted on which factors affecting the adoption of cloud computing in the organisation (Low et al., 2011; Morgan & Conboy, 2013 and Lian et al., 2014). However, cloud computing adoption by the organisations can be considered as a utopia, if individual users are not familiar with the new cloud technology. Sharma et al. (2016) point out studies from the field of information systems where behavioural constructs are critical factors influencing the individual user to adopt new technology (Al-Somali et al., 2009; Davis, 1989; Sharma and Govindaluri, 2014; Venkatesh et al., 2003). Sharma et al. (2016) examine if and into what extent factors such as perceived usefulness, perceived ease of use, computer self-efficacy and trust can affect individual users to adopt cloud technologies and indicates that the above factors were found to be significant indeed.

A major inhibiting factor has to do with the loss of control over storage of critical data and the service’s outsourced nature. The challenge for cloud providers is to identify and understand the concerns of privacy-sensitive stakeholders and adopt security practices that meet their requirements (Brunette and Mogull, 2009). Misunderstanding the privacy concerns of end users may lead to loss of business, as they may either stop using a perceivably insecure or privacy-abusing service or falsify their provided information – hence minimising the potential for profit via personalised advertising. An end user can give false data if she believes that the service provider is going to abuse the privacy agreement and sell personal data derived from a cloud-based subscription to a third party.
Samarati and Vimercati (2016) underline that the significant benefit of elasticity in clouds appealed companies and individual users to adopt cloud technologies. At the same time, this advantage is proved as harm to users’ privacy as security threats, and a potential loss of control of the owners of the data exists. In this case, the adoption and acceptance of the cloud computing paradigm is reduced. ENISA (2009) lists the topic of loss of control over data as a top risk for cloud computing. Also, in 2013 the “Cloud Security Alliance - CSA” contains data breaches and data loss as two of the main nine threats in cloud computing. The new complexity of the cloud paradigm (e.g. distribution and virtualisation), the class of data (e.g. sensitive data) or the fact that CSPs might be not entirely trustworthy are topics that increase security and privacy threats for cloud adoption.

Game theory in these cases emerges as an interesting tool to explore, as it can be used to interpret stakeholder interactions and interdependencies across the above scenarios. For example, Rajbhandari and Snekkenes (2011) implemented a game theory-based approach to analyse risks to privacy, in place of the traditional probabilistic risk analysis (PRA). Their scenario builds on an online bookstore where the user has to subscribe to have access to a service. Two players take part in this game: the user and the online bookstore. The user could provide either genuine or fake information, whereas the bookstore could sell user’s information to a third party or respect it. A mixed strategy Nash equilibrium was chosen for solving the game, with user’s negative payoffs, to describe the level of privacy risk quantitatively.

Snekkenes (2013) applies Conflicting Incentives Risk Analysis (CIRA) in a case where a bank and a customer are involved in a deal. Snekkenes attempts to identify who is to take the role of the risk owner in the event of data breach incidents and what are utility factors weighted on the risk holder’s perception of utility. The CIRA approach identifies stakeholders, actions and payoffs. Each action can be viewed as a strategy in a potentially complex game, where the implementation of the action amounts to the participation in a game. CIRA shows how this method can be used to identify privacy risks and human behaviour.

Also, according to Hausken (2002), the behavioural dimension is a critical factor to estimate risk. A conflict behaviour, which is recorded in individuals’ choices, can be integrated into probabilistic risk analysis and analysed through game theory. Friedman and Resnick (2001) worked on providing the use of “cheap pseudonyms” as a way to measure reputation in Internet interaction between stakeholders. This was a game of M players where users provided pseudonyms during an interaction in the Internet world, and they had the option either to continue playing with the current pseudonym or find a new one, at each period. A suboptimal equilibrium is found, as a repeated prisoner’s dilemma type of game, while methods of limiting identity changes are suggested.
Cai et al. (2016) insert a game-theory approach to manage decision errors, as there is a gap between strategic decisions and actual actions. They study the effects of decision errors on optimal equilibrium strategy of the firm and the user. Cavusoglu & Raghunathan (2008) propose a game theory for determining if a provider should invest in high or low-cost ICT and compare game theory and decision theory approaches. They show that in cases where firms choose their action before attackers choose theirs (sequential game), firms gain the maximum payoff. Also, when firms adopt knowledge from previous hacker attacks and uses learnings to estimate future hacker effort, then the distance between the results of decision theory and game theory approaches is diminishing.

Gao and Zhong (2016) address the problems of distorted incentives for stakeholders in an electronic environment, applying differential game theory in a case where two competing firms offer the same product to customers, and the one can influence the value of their information assets by changing pricing rates. To assure consumers that they do not risk losing sensitive information, and also, increase consumer demand, firms usually integrate their security investment strategies. Researchers reveal that higher consumer demand loss and higher targeted attacks, avert both firms from aggressive defence policy against hackers and would instead prefer to decrease the adverse effect of hacker attacks by lowering their pricing rates.

Concluding, game theory research in online privacy-related decision-making has shown that it can give credible results in understanding privacy-related behaviour.

5.3.4 The Basic Model

Decisions for storing and gathering information between the participants are made. Much importance is given to understanding the underlying motivations of their actions and reactions. In these decisions, risk and uncertainty are involved, and in this case, economic factors related to costs per processing, costs per unit of memory, costs per unit of storage and costs per unit of used bandwidth have to be taken into account (Calheiro, 2009). We develop a basic game model to understand how strategic interactions among the rational agents influence their behaviour to use or not such cloud services. Consider a cloud service provider (SP), i.e. a company which provides the ability to end users to store and share their data with others via mobile apps that enable data access and storage in a cloud computing environment. The company’s objective is to maintain a platform that can provide security services to end-users, while ensuring at the same time that profit is raised by delivering value for which clients are happy to pay, or at least surrender their personal data, for.

The SP stores personal information of end users in a database server, and an application server hosts some data reporting and monitoring applications using a remote mobile client over the
Internet. A two-tier service is provided: (a) free of charge with personalised advertising based on the retained personal data, or (b) paid for, which is advertising-free and offers greater sharing storage capacity.

The end user reads carefully and checks the privacy policy and decides to proceed with either registering for the free of charge option, consenting to their personal data being used for advertising purposes, or chooses the advertising-free, paid option. SP and end user then have an agreement. However, both of them have the opportunity to violate the agreement. The SP may use end users’ information in a more profit-making way that violates its privacy policy, e.g. passing the information to advertisers. The end user, on the other hand, may provide false personal information. That means that the end user is protected from privacy violations, but loses any personalisation advantages.

We assume that the case that someone registers for a paid service under false personal data is of equal payoff to the provider with the one where the data is accurate, as in this case the registered data would not be further used under SP’s consent. At that point, each party has to choose a strategy, based on their expectations of the other party’s behaviour. Therefore, exploring each party’s behaviour separately would not allow us to understand the dynamics of the SP - End-User interaction.

A game with a single end user and a service provider interacting is modelled below. Each player has the following options: to Cooperate (C) or to Defect (D). Cooperation for the end user is equal to providing accurate personal data while defecting is deciding to false personal information. Respectively, SP cooperates when she complies with privacy policies, while she defects when violates them. Thus, four combinations (strategy profiles) exist, which are presented in the following paragraphs together with our definitions of their corresponding payoffs.

The payoffs are in utility, and each strategy is given by the following simple formula: payoff = usage for internal purposes + selling information to third parties. If both end user and SP decide to defect, the end user receives a minimum benefit, and the SP may get some minimum benefit too if they manage to trade the false data, albeit inaccurate. We give it a value of one (1) for both in an arbitrary way.

If the end user is the actor who defects, while at the same time the SP respects the privacy policy, then the end user again gains some benefit (1), but the SP will get no benefit from providing the free service plus the cost of maintaining the privacy policy. Thus, we consider the payoff for the SP to be less than in the previous case, so we give it the value of zero (0).

If the end user gives real information about her and the SP mistreats it in some way, then the SP gains a significant profit, and the end user suffers a loss, as we indicated that we have a
privacy-sensitive end user. A payoff of three (3) is considered for the SP and (0) for the end user.

Finally, if both parties cooperate, then all will have benefits. The end user will receive personalised services according to their preference, and the SP may have the chance to use end user’s data, within the limits of the privacy policy. A payoff of two (2) is considered appropriate in such case to both players. The game is played in normal form and is being presented in Table 1. As we stated, we use arbitrary values for the payoffs for illustrative reasons. Only the order of payoffs is significant for the analysis that follows and not their exact values.

Defecting is thought to be a dominant strategy for SP as she wins a better payoff regardless of the end user’s choice. We are thus going to examine only how the end user would respond to the only remaining SP’s strategy (defect), as, from a privacy-concerned perspective, we can eliminate the dominated strategy for SP (cooperate). In this case, the end user will also defect. Thus, the equilibrium in the above game – the iterated dominant strategy equilibrium- is equal to {Defect, Defect}. In the equilibrium state, the overall payoffs are less than when both players cooperate.

Supposing that this game is played only once, we address the most straightforward format of the game. In fact, an SP would normally expect the end user to choose the same SP again and make a new subscription for data storage services. So, if the game is repeated there are two more factors to take into account. First, if there are finite or infinite repetitions and second if SP’s policy violation gets detected. If policy violation does not get detected, then the iterative version of the game is identical to the one-off game presented above. So, we only examine the case of apparent policy violation, i.e. one that gets immediately detected.

Referring to the finite case, the game is designed to be repeated several times and then stops. If we want to find a solution for this game, then we should first examine the last round. We can see that the game played in the last round is identical to the one we presented above. Thus, the end user would think that the SP would violate the policy the last time the game is
played. However, for the end user, it would be too late to fake her information. So, if the end user expects that at some time in the future the SP will mistreat the information provided, then she will fake her information from the beginning. Thus, the equilibrium of the finite repeated game is the same as in the case of the one-off game.

When an end user respects cloud services policies that consider reliable and makes regular moves, we may model the proper game as an infinitely repeated game. The case of the infinitely repeated game is more complicated. However, we can simplify our analysis, if we consider the act of discontinuing the end user-SP relation as a penalty imposed by the end user to the unreliable SP. The penalty is equivalent to the loss of profit from all future subscription fees or targeted advertising revenue.

While formal analysis of the game is left for future research; our preliminary analysis shows that defecting the privacy policy is a dominant strategy for the SP. Finally, the equilibria of the different variations of the end user-SP cloud privacy game are summarised in Table 5.4.

| Observable violation | One-off | Repeated | Infinitely repeated |
|-----------------------|---------|----------|---------------------|
|                       | D, D    | D, D     | C, C                |
| Undetectable violation| D, D    | D, D     | D, D                |

5.4. Equilibria in Variations of the End user-SP Privacy Game in Clouds

[5.3.5] Results

Below we will present some preliminary results from the above game model. Where end users can choose a cloud service provider to match their expectations, their stated privacy policies cannot assure trust. The utilisation of cloud computing services, such as in the content delivery domain is growing. However, it is still tough for many end users to trust service providers and store their personal data in a cloud-based environment, as privacy violation issues may perceivably happen at any time.

When end users adopt cloud-based services and chose to use compatible apps, they do not know in advance, if the service provider is reliable concerning retention of their personal data. There are many instances where end users provide false personal information to receive services (e.g. cloud-based storage) as they feel more protected. On the other hand, service providers are interested in implementing their strategic policies so that end users would remain loyal and pay for premium services. In this case, they should carefully consider giving data to a third party to avoid disappointing both their premium and basic end users and salvage their reputation.
Providing a fair solution to assure both end users’ loyalty and SP compliance is required. However, since such violations are difficult to be detected by most stakeholders, regulating the use of policies by enforcing audits is rather of low effectiveness. Imposing penalties for any violation from SPs or using reputation systems are effective countermeasures that assure end-users. SPs might not risk illicitly offending personal data when they are expected to lose some potential end users from such practices.

To summarise, we note that the above findings are applicable only to end users that care about privacy policies and are sensitive to privacy violations. Other end users may not behave in the same way, either because they believe that Internet users, in general, cannot effectively protect their privacy, or because they think that the information they reveal is not useful for further use by the SP or other third parties.

[5.3.6] Discussion and Future Research

A game-theoretic model has been developed to demonstrate that privacy policies alone are not enough to ensure that no violation would occur when an end user trusts free mobile apps in clouds. Equilibrium in this game comes when the SP does not adhere to the privacy policy and the end user fakes personal information.

Therefore, imposing penalties for violating SPs, or employing reputation systems that increase the cost of violation have to be considered to enforce policies that serve the purpose for which they were designed. It is also evident from our model that it is better for SPs and end users to be honest when they interact with a system.

We should also note that our ongoing study has limitations at this stage, as some potentially significant factors have been excluded from discussion in this paper. We have not presented the definition and analysis of our game model in the full formality of economic theory, as they are left for future research. There are also some limitations concerning the analysis of uncertainties underlying the players’ preferences. If players think differently, they will choose a different strategy, and a different equilibrium will occur.

Game theory is regarded as an excellent tool for behavioural analysis (Hausken, 2002; Rajbhandari & Snekkenes, 2011 & 2001) as rational agents interact in many fields of social life. There are many cases where privacy-related incidents obliged organisations to remove their products from the market with the considerable financial loss. It would be of value to provide guidance on how to consider such issues during risk analysis, to identify this kind of business risk from an SP’s perspective. Risk assessment, as a way to predict the likelihood of a threat occurs and the scale of its consequences, is not enough to provide much guidance on how to do this well. Game theory can be a fitting complement, as it is compatible with traditional risk management and could be integrated into approaches like PRA. Further work would be
focused on matching the ISO/IEC 27005 process (Rajbhandari & Snekkenes, 2011) with complimentary game theory techniques.

5.4. Consumer Trust in Cloud Services and the Role of Security Certification: A Game-Theoretic Analysis

5.4.1 Impact of Consumer Trust in Cloud Services

Sato (2010) refers that 88% of consumers, worldwide, are worried about the loss of their data. Who has access to their data? Where consumers’ data is physically stored? Can cloud service providers (CSPs) find ways to gain consumers’ trust? Is the CSPs attempt towards consumer trust, value for money strategy? These are typical questions that consumer and CSPs make about trust in clouds and online environments.

Ramachandran and Chang (2016) provide fundamental issues associated with data security in the clouds. One key factor for cloud adoption is building trust when storing and computing sensitive data in the cloud. Consumers have limited control over their data. Security concerns arise as consumers do not store data in their premises and also, the multi-tenancy feature of the cloud increases the risk of data breaches.

Trust related to e-services offered in virtual online environments is a major topic for both consumers and cloud service providers, as well as for cloud researchers. Trust is firmly tied to online security. McKnight et al. (2002) indicate three significant trust components: ability, integrity and goodwill as prominent factors for a new ICT adoption. Ability is equal to CSPs efficiency in resources and skills that will not deter consumers from adopting cloud technologies. Integrity refers to CSPs obligations to comply with regulations, and goodwill means that CSPs assure priority to consumers’ needs.

Sharma (2016) suggests that trust in clouds has a positive and significant relationship with individual’s decision to adopt cloud computing services. In clouds, users often want to share sensitive information, and CSPs should ensure their privacy (King & Raja, 2012). Svantesson and Clarke (2010) suggested that CSPs apply such policy to ensure users that their data are safe and allure them to use clouds.

Consumers trust CSPs only to the extent that the risk is perceived to be low and the convenience payoff for them high. Pearson (2013) argues that when customers have to decide about trusting CSPs for data exchange services, they should consider organisation’s operational, security, privacy and compliance requirements and choose the best suit them.
ISMS implementation and the role of security certifications in clouds

An information security management system (ISMS) refers to policies about information security management that help organisations to manage risks related to information security. ISO/IEC 27001:2013 is a risk-based information security standard that incorporates the «Plan-Do-Check-Act» (PDCA) approach and implements ISMS as follow (Humphreys, 2011):

- **The Plan** is the ISMS designing phase, which assesses information security risks and selects the appropriate controls.
- **The Do** refers to implementing and operating the controls phase.
- **The Check** is a review and evaluation ISMS phase.
- **In the Act phase**, the appropriate changes are made in order ISMS ensure security level in the best way.

Cloud services can be considered as an additional layer to IT infrastructure. Within the context of information technology and regarding information security and compliance, certificates are an established mechanism to create trust between a service provider and a potential consumer (Humberg and Jürjens, 2016). Certificates can be distinguished by their domain:

- a) General information security standards and certificates (e.g. ISO/IEC 27001:2013);
- b) Cloud-specific certificates (e.g. ISO/IEC27018);
- c) Domain-specific certificates (e.g. FedRamp)

In July 2014 a new standard for public cloud computing and data protection was published. Hert et al. (2016) refers to “ISO/IEC 27018:2014 - Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”, as a guidance for ensuring that cloud service providers offer suitable controls to protect consumers’ privacy by securing PII (Personally Identifiable Information). “ISO/IEC 27018 is the first standard on cloud computing that deals with personal data protection and published at a very critical period when cloud computing is considered as the solution for many companies to reduce operational costs and for consumers to trust their personal data in virtual and easy accessible environments.

Cloud computing combines several benefits such as minimising cost, ease of use, and simplicity as it is regarded as a significant conjunction of the best of grid computing and service-oriented computing. A trust management framework for clouds can help researchers provide solutions in areas, such as identification, privacy, personalisation, integration, security, and scalability challenges (Noor et al.,2016).

Trust management from the service provider perspective is related to the obligation to provide consumers’ trustworthiness, or from consumers request to CSPs to assess trustworthiness. Policies, recommendations, reputation, or prediction are a requisition in any
case. The best way to establish trust among independent entities is to control end-user authorisation through a policy.

ENISA (2009) consider cloud computing as a new way of delivering computing resources and not a new technology. A top recommendation introduced by ENISA is the assurance for cloud customers. CSPs follow security practices in mitigating risks that customers and providers are afraid of. They use this knowledge to make sound business decisions and maintain or obtain security certifications. Hence, the need for assurance translated into the need for cloud providers to be audited. For this reason, ENISA provides a check-list with all aspects of security requirements including legal issues, physical security, policy issues and technical issues for CSPs to obtain assurance. More precisely the check-list involves: “Assess the risk of adopting cloud services; Compare different cloud provider offerings; Obtain assurance from selected cloud providers; Reduce the assurance burden on cloud providers”. Solutions to privacy and security in cloud computing include policy and legislation as well as end users' choices for how data is stored.

CSPs have to confirm to regulations, certifications and standards as compliance and certification cover not only Information Security (IS) standards and compliance but also, auditing recommendations (Gapinski, 2015). Certifications and assessment by external agencies in the areas of Information Security, compliance with regulations, and auditing are guarantees for CSPs business strategy as far as for customers' assurance.

Humberg & Jürjens (2016), Figliola & Fischer (2015) and Yiman & Fernadez (2016) are working on Compliance in Clouds. They infer that information technology leverage for business operations is tied to considerations about compliance and security assurance in clouds. Noor (2011) indicate that trust management is highly recognized in clouds as a way to assess and manage trust feedbacks collected from participants. Hwang & Li (2010) and Conner et al. (2009) suggest that cloud security infrastructure and trust management will play a significant role in leveraging cloud services.

Kumar and Pandey (2016) set the question: “Would cloud providers and clients have custody battles over client data?” Privacy and control cannot be solved entirely in public clouds but assured with service level agreements (SLAs) between the service provider and the service user.

From the research reviewed, it is inferred that cloud computing has become a leading service in the online world. With the cost parameter being a unique advantage, CSPs use cloud-computing increasingly to reduce operational cost, to boost flexibility, and ensure data storage (Raisinghani, 2015).
Cost/Benefit Analysis in Clouds

Cost-benefit analysis (CBA) is a systematic process used to determine options, calculate and compare advantages and costs of a proposed “good.” and decided on it (Cellini and Kee, 2010). Cloud economics as presented in this section refer to the economic forces and structural issues affecting the costs and benefits of adopting the cloud technologies. A cost-benefit analysis identifies values on the costs of adopting clouds, but it goes further, weighing those costs against values of cloud benefits. Regarding analysis, analysts deduct costs from benefits to obtain the net benefits of the policy (negative net benefits refer to net costs): \[ \text{Net Benefits} = \text{Total Benefits} - \text{Total Cost}. \]

Cloud computing features such as elasticity, scalability, low entry cost, motivate consumers to migrate their personal data to the cloud (Yimam & Fernandez, 2016). In the same tone, Mell and Grace (2009) underline benefits such as cost-savings, power savings, green-savings and flexibility as a good reason for organisations and consumers to adopt cloud computing technologies.

Cloud computing gain benefits of a web-based infrastructure where services are developed massively and almost costlessly, without the expenses of in-house storage infrastructure (Jhang-Li and Chiang, 2015; Wu et al., 2013; Zorrilla and García-Saiz, 2013). Even though much research was conducted in the cloud computing area, the majority of this research focuses on clouds conceptualisation. Some empirical cloud computing studies were done on the adoption of cloud computing (e.g., Wu et al., 2013), while less empirical research has done in associating cloud computing with the economic or environmental performance, taking into considerations marketplace standards and key competitors.

The potential financial cloud-benefits arise from the fact that resources such as hardware and software are provided without the need to purchase additional infrastructure. Consumers have access remotely at any time and relatively low cost (Figliola & Fischer, 2015). The literature reveals that cost reduction occurred by migrating to clouds in a key factor for businesses efficiency and consumers satisfaction. Moving to clouds is a strategy for businesses to alleviate investment cost additionally in hardware and infrastructure as they pay only for the number of computer resources and services they use. Also, consumers pay only for the computing resources that they consume (Armbrust et al., 2010; Han, 2010; Kim, 2011; Zhang et al., 2010).

Kash and Key (2016) suggest that in simple economic terms, cloud service providers shape an oligopoly. Consider the case where Microsoft has decided to adopt the same price policy with Amazon for basic infrastructure. In this case, both providers are expected to find ways such as providing personalised enriched services to gain a competitive advantage the one over the other. Thus, consumers enjoy higher value services and service providers transfer the
potential profit to build market share in the commodity market. The use of price discrimination that charges different amounts for the same products, as a way to create added value and increase revenue is a common method. The equilibrium pricing in the above oligopoly case reminds Cournot equilibrium as Microsoft and Amazon produce a homogeneous product, they do not cooperate, they have market power and the output of one decision affect the asset’s price. They act strategically as economically rational agents who are seeking to maximise profit given their competitors’ decisions.

Pricing the cloud is not like pricing electricity. It is not easy to measure and estimate precisely clouds value. For this reason, a cloud utility model is adopted where good like electricity can be used as an example to measure and charge a unit per use.

Schniederjans and Hales (2016) consider cloud computing as an online IT resource that has an added value varies depending on the type of service, payment options and personalisation strategies. The most common services that are used by the consumer are software-as-a-service (SaaS) and lesser platform-as-a-service (PaaS) and infrastructure as a service (IaaS) (Doelitzscher, 2011). Price discrimination and privatisation include payment options include elastic or pay-per-minute models or fixed and subscription-based pricing.

At this point, it is understood that Computer Sciences, Game Theory and Economics are combined as an attempt to interpret the above forms of discrimination policies and ensure the cloud economics future research.

[5.4.4] Asymmetric Information and Strategic Stakeholders Interaction in Clouds: A game theory approach based on trust

Asymmetric information is a concept often encountered in commercial transactions between sellers and buyers, end-users and service providers where the one party has more information compared to the other. Potentially, this could lead to a harmful situation as the one party can take advantage of the other party’s lack of knowledge. Information asymmetries are commonly met in principal-agent problems where misinforming caused and the communication process is affected (Christozov et al., 2009).

Principal-agent problems occur when an entity (or agent) makes decisions on behalf of another entity: the "principal – a person, who authorises an agent to act with a third trusted-party"(Eisenhardt, 1989 and Bosse & Phillips, 2016). A dilemma exists when the agreement between participants is not respected, and the agent is motivated to act for his gain and in contrary to the “principal”. Principals do not know enough about whether an agreement has been satisfied and therefore their decisions are taken under some risk and uncertainty and
involve costs for both parties. The above information problem can be solved if the third trusted-party provides incentives so as the agents to act appropriately and by the principals. Regarding game theory, rules should be changed so that the rational agents confronted with what principal desires (Bosse & Phillips, 2016).

McKinney and Yoos (2010) refer that information is almost always unspecified to an infinite variety of problems and the involved agents (so-called stakeholders) almost always act without having full information about their decisions. While the literature on information risk is adequately studied in the last decades; there is no risk premium for information asymmetry (Hirshleifer et al., 2016). Easley and O’Hara (2004) argue that information asymmetry creates something called information risk and their model showed that more private information from consumers receives higher expected returns to the involved agents.

For an agent, a risk premium is the minimum economic benefit by which the expected return from a decision-making under risk must exceed the known return on a risk-free decision where full information is provided to the involved stakeholders. It is positive if an agent is risk averse, namely when he exposed to uncertainty caused by information asymmetry, to attempt to reduce that uncertainty. The utility of such a strategic movement expected to be high in many cases. For such risky outcomes, a decision-maker adopts a criterion as a rule of choice, where higher expected value strategic movements are simply the preferred ones (O’Brien and Ahmed, 2016).

From a game theory perspective, uncertain outcomes exist potential preferences with regards to appropriate risky choices coincide. In cases where the above-expected utility hypothesis is satisfied, it can be proved useful to explain choices that seem to differ from the expected value criterion. Asymmetric information in clouding introduces scenarios where stakeholders (consumers and service providers) interact strategically. A game theory approach based on trust is regarded as a useful tool to explain the conflict and cooperation between intelligent, rational decision-makers.

Public clouds considered as a great advantage for stakeholders regarding flexibility, scalability and cost-effectiveness. Despite the advantages, the feature of public clouds subject to security issues and challenges according to data control, which remain unresolved. Njilla et al. (2016) introduce a game theoretical modelling for trust in clouds suggesting that risk and trust are two behavioural factors that influence decision-making in uncertain environments like cloud markets where consumers seem not to have full control over their stored data. They adopt a game theoretic approach to establishing a relationship between trust and factors that could affect the assessments to risk. The scenario refers to three players: end-users, service providers, and attackers. Provider defends the system’s infrastructure against attackers, while end-users tempt not to trust an online service in case of data privacy breaches. Njilla et al. (2016) propose a game model which mitigate cyber attack behaviour in security.
implementation. They analyse different solutions obtained from the Nash equilibrium (NE) and find that frequent attacks with contemporary providers’ ability to mitigate the loss, might cause the attacker to be detected and caught. Thus, it is possible in that case attacker not attack because of high risk and penalties. However, what about the gain and the loss when the provider invests in security, and the attacker decides to attack and succeeds his target with users’ private data compromised? What are the payoffs of each player in this case? This regarded as an open question.

Maghrabi and Pfluegel (2015) use game theory from an end-user perspective to assess risk since moving to public clouds. While previous works focus on how to help cloud provider to assess risk, they develop a model for benefits and costs associated to attacks on the end-user’s asset to help the user to decide whether or not adopt the cloud. The end-user is conformed to a Service Level Agreement (SLA), which promises to protect against external attacks. The writers suggest that they can use the degree of trust $T$ that a user has in a cloud provider. Pure Nash equilibrium exists for values $T = 0$, and $T = 1$ and Maghrabi and Pfluegel compute a mixed Nash equilibrium in the case where $T$ is between 0 and 1. The above user-centric game model using the notion of trust results to a pure Nash equilibrium for completely trusted cloud provider and complete lack of trust in the provider.

Douss et al. (2014) propose a game trust model for mobile ad hoc networks. Assuring reputation and establishing trust between collaborating parties is indirectly a way to provide the secure online environment. The authors suggest an evaluation model for trust value. They applied computational methods and developed a framework for trust establishment.

Li et al. (2016) study price bidding strategies when multiple users interact and compete for resource usage in cloud computing. The provided cloud services are available to end-users in a pay-as-you-go manner (Kaur and Chana, 2014; Pal and Hui, 2013). A non-cooperative game model is developed with multiple cloud users, where each cloud user has incomplete and asymmetric information about the other users. They work on utility functions with the “time efficiency” parameters incorporated to calculate net profit for each user, to help them to decide whether to use the cloud service. For a cloud provider, the income is the number of money users pay for resource usage (Mei et al., 2015). A rational user will maximise his net reward by choosing the appropriate bidding strategy $(U_{\text{of choosing the cloud service}} - P_{\text{ayment}})$. However, it is irrational for a cloud provider to provide enough resources for all potential requests at a specific time. Therefore, cloud users compete for resource usage. The above stakeholders’ strategic interactions are analyzed from a game theoretic perspective, and the existence of Nash equilibrium is also confirmed by a proposed near-equilibrium price bidding algorithm. For future research, the good idea is to study the cloud users’ choice among different cloud providers or determine a proper mixed bidding strategy.
Fagnani et al. (2016) consider a network of units (e.g. smartphones or tablets) where users have decided to make an external backup for their data and also, can offer space to store data of other connected units. They propose a peer-to-peer storage game model and design also, an algorithm which makes units interact and store data back up from connected neighbours. The algorithm has been converged to Nash equilibrium of the game, but several challenges have arisen for future research analysis related to stakeholders interactions in a more trusted environment.

Moreover, the resource allocation problem in cloud computing where users compete for gaining more space to run their applications and store their data is analyzed by Jebalia et al. (2015). They develop a resource allocation model based on a cooperative game approach, where cloud providers provide a significant number of resources to maximise profit and combine the adoption of security mechanisms with payoffs maximising.

Security and privacy are often located as different concepts. Much of focus is on reducing cost during the establishment of a trust-worthiness infrastructure in cloud computing, which gradually requires disclosing private information and proposing a model of trading privacy for trust (Seigneur and Jensen, 2004; Njilla et al., 2016). Also, Lilien et al. (2008) indicate the difference between maintaining a high level of privacy and establishing a trust for transactions in cloud environments. Users, who display a particular interest in concealing private information intensively, request from cloud providers a set of corresponding credentials which establishing a trust for these users. The tradeoff problem exists where the assurance for the minimum user’s privacy loss meet the choice of revealing the minimum number of credentials for satisfying trust requirements.

Raya et al. (2010) suggest a trust–privacy tradeoff game theoretical model that gives incentives to stakeholders to build trust and at the same time assure privacy loss at a minimum level. Individual players would not trust cloud providers unless they received an appropriate incentive.

Gal-Oz et al. (2011) introduce a tradeoff approach studying the relationship between trust and privacy in online transactions. They suggest that pseudonyms constitute a necessary component for maintaining privacy since pseudonyms prevent association with transaction ID and ensure a level of reputation. The more pseudonyms used, the more reputation is succeeded.

Following major problems has been observed during the study we indicate that any application relying upon an emerging cloud computing technology should consider the different possible threats. The problem is a lack of a clearly defined meaning of such a risk that benefits the cloud users to make proper choice and cloud service providers to avoid threats efficiently.
5.4.5 Overview of the study

Cost and benefit analysis over personal data indicates practices from both stakeholders. The numerous benefits of cloud services have enticed individuals and enterprises who are massively moving towards the cloud paradigm. Universal data access, scalability, avoidance of expenditure on hardware and software, and relief of the burden of storage management are some of the alluring benefits of cloud computing. However, as more and more information on individuals and enterprises is placed in the cloud, security and privacy concerns are growing (Yadav et al., 2012).

Estimating the benefit-to-risk ratio of using cloud services is a challenging task. Potential consumers of cloud services do not have direct access to or detailed information about the cloud service provider’s infrastructure and the security measures implemented. As a result, they are not able to estimate risk, and they have to rely on the CSP claims. Thus, asymmetry in information available to CSPs and consumers is introduced.

Consumers expect CSPs to implement an efficient Information Security Management System (ISMS), which would ensure a level of protection analogous to the risks associated with the cloud service. Nevertheless, consumers are not able to inspect the appropriateness and effectiveness of the ISMS. If the CSP is a weak security implementer or if the CSP stops investing in security at some point would only become known to the consumer after a security breach has occurred. Historical data provide little information to the consumer. First, because the absence of security breaches in the past could be due to contingent factors. Second, because almost all providers that have suffered security breaches in the past claim that they have improved their security to mitigate the chances that a similar incident happens in the future. So, the consumer, again, has to make a decision based on CSP’s claims.

The above characteristics place cloud services in a category of goods and services referred to as experience goods in the economics literature (McCluskey, 2000). With experience goods, quality can only be determined after the product has been purchased. In the case of cloud services, the ineffectiveness of data protection might be detected long after the consumer uses the cloud services when the damage is probably irreversible. The categorisation of goods about the knowledge of quality characteristics at the time of purchase also includes search goods and credence goods. In the case of search goods, there is perfect information about quality before purchase, while with credence goods quality cannot be directly observed. Examples of credence goods are organic foods, dolphin-safe tuna and free-range meat (McCluskey, 2000). For example, it is impossible for consumers to determine if the tuna they consumed has been fished with methods that don’t hurt dolphins, although some consumers
may find this very important for ethical reasons and might be willing to pay higher prices for dolphin-safe tuna.

Information asymmetry often leads to lemons markets. A lemons market is a market where only goods of low quality are sold because consumers would not pay higher prices for products that are presented as higher quality, but without any assurance that the claim is valid. Previous research has shown that information privacy is a lemons market (Vila et al., 2003). However, this and other similar works (Anastasopoulou et al., 2013) examine provider’s compliance with its public security policy and undeclared secondary usage of data. In this paper, we focus on the effectiveness of data protection, and we leave deliberate violation of security policy out of scope.

A way to resolve the issue of asymmetric information is to engage third-party assurance. The above usually implies a certification scheme. In the case of information, security ISO provides such a scheme based on the ISO/IEC 27001 standard (ISO, 2013). ISO/IEC 27001 specifies the requirements for Information Security Management Systems. Companies can be certified against ISO27001 by one of the accredited bodies.

This study aims to examine how asymmetric information on the security system implemented by the CSP affects the strategic choices of CSPs and consumers. Moreover, we examine the role of security certification and how it may change the strategic choices of consumers and CSPs.

[5.4.6] The Basic Model

Cloud services as an experience good

To illustrate the effects of information asymmetry we first consider a simple game-theoretic model with two players, the CSP and the Consumer. The game designed in an extensive form is depicted in figure 1. The last row of the game tree in figure 1 shows the payoffs of the two players in parenthesis. On the left, it is CSP’s payoff and on the right consumer’s payoff. CSP’s payoff is in monetary units, while consumer’s payoff is regarding utility. These correspond to the purchase of one unit of service, which could be the standard contract or a standard subscription.
We define the following variables:

- \( P \): CSPs profit from delivering cloud services
- \( C \): CSPs per unit cost for implementing and efficient ISMS
- \( B \): Consumers benefit from purchasing cloud services
- \( L \): Consumer's loss from a security breach

In this model the CSP has two strategic choices: (a) to implement an effective ISMS, (b) not to implement an effective ISMS. The consumer has two options: (a) to purchase cloud services and (b) not to purchase cloud services. However, at the time of purchase, the consumer does not know whether the CSP has implemented or not the ISMS. The above is shown in Figure 1 with the dotted lines that define an information set.

Although no security system could guarantee 100% security, we assume that an ISMS compliant with ISO27001 would provide a level of security equivalent to the one the consumer would implement if he/she chose the in-house solution. In other words, the ISMS would make the consumer security-wise indifferent in his/her choice to go for the cloud.

About the payoffs, the consumer would have a benefit of \( B \) if he/she purchases cloud services from a provider that implements an efficient ISMS. Otherwise, if the CSP does not provide adequate security, then consumer’s payoff is reduced by \( L \), i.e. the loss resulting from a security breach. In this basic model, we assume that a security breach will certainly happen if there is no adequate security in place. This assumption is removed in subsequent enhanced models. If the consumer does not buy, then the payoff is equal to zero, meaning that he/she does not lose or earn anything. From the CSPs side, profit \( P \) is reduced by the cost of
implementing and maintaining an effective ISMS, which is marked as C. If the CSP implements ISMS and the consumer doesn’t buy, then the CSP has a loss that equals C. If the CSP doesn’t implement ISMS, it gets a profit of P when the consumer buys and a profit of zero when the consumer doesn’t buy.

If the CSP and the consumer interact only once, then they are playing a single stage game. In the stage game if \( B \geq L \) the strategic profile (No ISMS, Buy) constitutes the only Nash Equilibrium. Otherwise, if \( B < L \) then (No ISMS, Don’t Buy) is an equilibrium. In other words, if the consumer values the benefits of cloud services as more important than the loss in case of a security breach, then he/she will purchase the services. There is no Nash Equilibrium in the stage game in which the CSP implements an effective ISMS. Consequently, all potential users of cloud services that have sensitive data are deterred from purchasing cloud services. This result is in line with the characterisation of security as a lemons market.

In most cases, a CSP would aim for a long-term relationship with customers. In this case, the CSP-Consumer interaction is modelled as an infinitely repeated game. In this case, the term \textit{infinitely repeated game} refers to a game that is repeated for an undefined period. In the repeated game, consumers have to choose whether to renew their subscription. This is equivalent to a new purchase of cloud services. Players in repeated games can follow complex strategies, which may depend on what the other player played in the previous periods. According to the “folk theorem” for repeated games if the players are sufficiently patient, then any feasible, individually rational payoff vector of the stage game constitutes a sub-game perfect equilibrium payoff in the associated infinitely repeated game.

We examine the case where \( B \) is less than \( L \), i.e. to consumers with sensitive data, since the rest would buy cloud services regardless of the effectiveness of their security measures, as we have shown above. Then, we shall examine if the following strategies are enforceable.

- **CSP**: Implement an effective ISMS and maintain it, if the consumer continues to buy. Otherwise, stop maintaining it.
- **Consumer**: Buy in the first period. Then, buy if ISMS is maintained, otherwise don’t buy.

These strategies are known as grim strategies in the relevant literature. An interesting point here is that the Consumer in several cases would experience losses long after a security breach has occurred. That means that there would be an extended period before the consumer makes the next informed decision on whether to continue his/her subscription or not. As a result, the periods in the repeated game are long, and the CSP would expect to benefit from subscriptions for an extended period before it gets penalised by consumers for inadequate security. This parameter is included in our model as a discount factor \( \delta_{sp} \), where \( 0 \leq \delta_{sp} \leq 1 \).
Future payoffs are discounted by $\delta_{sp}$, which means that profit $P$ in the next period counts $\delta_{sp}$ $P$ in this period.

A CSP would sustain the grim strategy if the present value of payoffs in this and all the following periods is greater in the case of sustaining the grim strategy than in the case of deviating. More specifically, the CSP would have no incentive to deviate if:

$$P < \sum_{t=0}^{\infty} \delta_{sp}^t (P - C)$$

5-1 Equation for CSP with no incentive to deviate

If the CSP decides to stop maintaining the ISMS, it will get a profit of $P$ the first period, but zero profits the next periods, after the consumer finds out. Otherwise, CSP would get a profit $P-C$ for this period and $P-C$ discounted by $\delta_{sp}$ all the following periods. Rearranging the factors, we get the following inequality:

$$\frac{P}{P - C} < \frac{1}{1 - \delta_{sp}}$$

5-2 CSP decides to stop maintaining the ISMS

A $\delta_{sp}$ close to zero means that the present value of future profits is low, which happens if it takes much time for the consumer to find out that the CSP provides inadequate security. The closer $\delta_{sp}$ gets to zero the smaller the right part of the inequality gets, which gives an incentive to the CSP to deviate from the desirable strategy. Therefore, a regulation that requires immediate disclosure of security incidents has a positive effect.

**Model extension with breach probability as a variable**

In the above game we assumed that when the CSP discontinuous maintaining an effective ISMS, a security breach will certainly happen. However, this is rarely a case. Systems with poor security may avoid breaches for a long period. Thus, we enhance our model with the parameter $p$, which is the probability of a security incident that may lead to a security breach if there is no effective ISMS installed. We assume that $p$ is known to both players. The game in extensive-form is presented in Figure 5-6.
Dotted lines represent information sets. We consider that although the CSP can estimate the incident probability $p$, they do not know if an incident will happen in the next period.

In the stage game if $p \leq \frac{B}{L}$

The strategy profile \{No ISMS, Buy\} constitutes an equilibrium. Otherwise, the equilibrium is \{No ISMS, Don’t buy\}. We notice that the CSP always chooses not to implement ISMS, as this is the dominant strategy, i.e. the strategy that has the higher payoff regardless of the other player’s actions. The consumer, knowing that the CSP has no incentive to implement effective ISMS, will buy if the probability of a security incident is less than the Benefit-to-Loss ratio. In other words, if either the likelihood of an incident is high or the potential losses are far more than the potential benefits, the consumer will avoid the cloud option.

Next, we shall examine the repeated version of the game. In the repeated version we shall examine the sustainability of the same pair of strategies, i.e.:

- **CSP**: Implement an effective ISMS and maintain it, if the consumer continues to buy. Otherwise, stop maintaining it.
• Consumer: Buy in the first period. Then, buy if ISMS is maintained, otherwise don’t buy.

The following table depicts the present-value payoffs for equilibrium case and the deviation.

|                  | Equilibrium Payoffs | Deviation Payoffs |
|------------------|---------------------|-------------------|
| CSP              | \(\frac{P - C}{1 - \delta_{sp}}\) | \(P + \frac{\delta_{sp}(1 - p)P}{1 - \delta_{sp}}\) |
| Consumer         | \(B\)               | 0                 |

5-1 Table 1: Present-value payoffs for repeated game

In the above table, we see that if the CSP sustains the strategy above, then they will get a payoff of \(P - C\) for all the following periods. The present-value payoff is calculated assuming a discount rate of \(\delta_{sp}\). In the case that the CSP decides to deviate from the strategy, then they will get a payoff of \(P\) for the first period and, then, with probability \((1-p)\) they will continue to have a profit of \(P\). If an incident happens, then their profit will be zero. In order the CSP not to have an incentive to deviate the following condition should hold:

\[
\frac{P - C}{1 - \delta_{sp}} > P + \frac{\delta_{sp}(1 - p)P}{1 - \delta_{sp}}
\]

5-3 CSP with no incentive to deviate from the strategy

This expression can be re-arranged as follows for a straightforward interpretation:

\[
\delta_{sp} p > \frac{C}{P}
\]

5-4 Present-value payoffs for repeated game

According to the above condition, the discounted probability of a security incident should be larger than the Cost-Benefit ratio. Thus, CSP shall maintain effective ISMS as long as the consumer continues to use the cloud service and there is a high breach probability that can’t be kept secret for an extended period, and the cost of security is small in comparison to the profits the CSP makes from consumers with sensitive data. In other words, in most cases, the CSP would take just those security measures that are more cost-effective and focus on security issues that would be directly detectable by consumers (e.g. system availability, hacking by outsiders, etc.) rather than implementing a thorough security policy as part of a comprehensive ISMS. [Much economic analysis can be done, based on his equation].
[5.4.7] The case of security certification scheme

In this section, we shall examine the role of security certification. Certification and third-party monitoring, in general, are common ways of resolving lemons-market deadlocks. For example, certification has been very effective in enabling an organic products market, where the consumer is not able to observe the production methods. In the case of information security, a popular standard is ISO27001 (ISO/IEC, 2013).

Nevertheless, no certification scheme is perfect, and there is always room for opportunistic behaviour, where CSPs may apply for a certificate although not fully compliant hoping to pass the audit, or they may relax the implementation of the ISMS between audits. Therefore, in the next game model, we distinguish between compliant and opportunist CSPs. Although the consumer cannot distinguish between the two, he/she may estimate the probability that the CSP is the compliant type being equal to $q$. We, also, assume that the probability that an opportunist CSP gets certified to be equal to $r$. Finally, the cost of applying for a certificate is equal to $K$. Again, a security incident may or may not happen with probability $p$. In Figure 3, we present the relevant game for the case that a security incident will occur. Consumer nodes with dotted rectangles of the same type belonging to the same information set. The game in the case that the security incident does not occur has the same structure, and it differs only in the payoffs, as shown in Figure 4.

In the analysis that follows we restrict to the case that $L > B$, since if potential losses are less than benefits, then the game has a distinct equilibrium: Consumer always buy and the CSP
never implements an ISMS. To determine consumer’s best response, we first examine the probability that CSP is Compliant if we know that CSP is certified. We name $E_c$ the event that the CSP is compliant, $E_{op}$ the event that CSP is an opportunist and $F_{cert}$ the event that the CSP is certified. According to Bayes’ theorem the probability that the CSP is compliant given that it has been certified is:

$$P(E_c|F_{cert}) = \frac{P(F_{cert}|E_c) \cdot P(E_c)}{P(F_{cert}|E_c) \cdot P(E_c) + P(F_{cert}|E_{nc}) \cdot P(E_{nc})}$$

5-5 Bayes’ theorem: the probability for CSP to comply

We consider that if the CSP is compliant and applies for a certificate, it will always get certified. So, if the probability of CSP to be compliant is $q$, and the probability that it gets certified when it is not compliant is $r$, then the probability that it is compliant given that it has been certified is:

$$P(E_c|F_{cert}) = \frac{q}{(1 - r)q + r}$$

5-6 When CSP is compliant and applies for a certificate

If the CSP is certified then consumer’s expected utility from buying is:

$$EU_c(F_{cert}) = P(E_c|F_{cert}) \cdot B + [1 - P(E_c|F_{cert})] \cdot (B - L)$$

5-7 Consumer’s expected utility when CSP is certified

The above applies when a security incident is bound to happen. If we consider $p$ the probability that an incident happens (i.e. the case in Figure 3) and $(1-p)$ the probability that an incident does not happen, then the expected utility is:

$$EU_c(F_{cert}) = P(E_c|F_{cert}) \cdot B + p[1 - P(E_c|F_{cert})] \cdot (B - L) + (1 - p)[1 - P(E_c|F_{cert})] \cdot B$$

5-8 The expected utility by the probability that an incident does not happen

By substitution, we get the following expression:

$$EU_c(F_{cert}) = B \left( \frac{q}{(1 - r)q + r} + p \left( B - L \right) \left( 1 - \frac{q}{(1 - r)q + r} \right) + (1 - p)B \left( 1 - \frac{q}{(1 - r)q + r} \right) \right)$$

5-9 Consumer’s decision to buy from a certified CSP

The consumer will buy from a certified CSP if $EU_c(F_{cert}) > 0$. As the only factor that may get negative value is $(B - L)$ we express the above inequality as follows:

$$B \left( \frac{q}{(1 - r)q + r} + (1 - p)B \left( 1 - \frac{q}{(1 - r)q + r} \right) \right) > p \left( L - B \right) \left( 1 - \frac{q}{(1 - r)q + r} \right)$$

5-10 Consumers benefit from purchasing and probability to lose from a security breach
Based on the above we can make the following observations. If \( p \) is considerably small, then the consumer will buy. Thus, we shall further examine the case where \( p=1 \). In this case, the consumer will buy if

\[
\frac{q}{(1 - r)q + r} > \frac{L - B}{L}
\]

5-11 If \( p \) is considerably small, then the consumer will buy.

The first part of the expression equals 1, when \( r = 0 \), i.e. when the audit procedure for the certification is flawless.

Assuming that the above conditions apply and \( EU_c(F_{cert}) > 0 \), then we examine CSPs best response. If CSP is of the compliant type, then they will apply if \( P > K \), i.e. if the cost for certification is not larger from the profit. If opportunist, CSP will be deterred from applying if \( r(P-K) + (1-r)(-K) < 0 \). The first part of the inequality represents CSPs payoff if applying, while the payoff if not applying is 0. By re-arranging the above expression, we get the following inequality:

\[
P < \frac{K}{r}
\]

5 12 CSPs best response 1

Thus, for the CSP strategy \{Apply if compliant, Don’t apply if not compliant\} to be the best response to a consumer that \{Buys if CSP is certified, Doesn’t buy if CSP is not certified\} the following condition should apply:

\[
K < P < \frac{K}{r}
\]

5-13 CSPs best response 2

We may observe that certification without cost would result in high opportunism, even if the certification process is flawless. High opportunism would again result in a lemons market situation. The upper limit for the certification cost is \( P \), if \( r < 1 \), which means that with marginally active monitoring, the certification process could drain almost all profits. However, if there is price competition amongst certifying bodies, then the certification cost would tend to fall. The issue, now, is how low it could fall? The answer is given by the inequality \( K > rP \), i.e. certifying bodies cannot sacrifice monitoring effectiveness for a reduced cost.
Results

We take a game-theoretic approach to explore the motivation of firms for privacy protection and its impact on competition and social welfare in the context of product and price personalisation. We find that privacy protection can work as a competition-mitigating mechanism by generating asymmetry in the consumer segments to which firms offer personalisation, enhancing the profit extraction abilities of the firms. In equilibrium, both symmetric and asymmetric choices of privacy protection by the firms can result, depending on the size of the personalisation scope and the investment cost of protection. Further, as consumers become more concerned about their privacy, it is more likely that all firms adopt privacy protection. In the perspective of welfare, we show that autonomous choices of privacy protection by personalising firms can improve social welfare at the expense of consumer welfare. We further find that regulation enforcing the implementation of fair information practices can be efficient from the social welfare perspective mainly by limiting the incentives of the firms to exploit the competition-mitigation effect.

E-commerce transactions, in addition to the exchange of goods and services for payment, often entail an indirect transaction, where personal data are exchanged for better services or lower prices. We analyse buyer’s and seller’s privacy-related strategic choices in e-commerce transactions through game theory. We demonstrate how game theory can explain why buyers mistrust internet privacy policies and relevant technologies (e.g. P3P), and sellers hesitate to invest in data protection.

Another reference and current research field are related to privacy concerns in Cloud Computing. Free mobile applications of cloud computing offer a range of diverse services (e.g. gaming, storage etc.) usually in return for delivering personalised advertising to their consenting end-users. To do so, they may retain a range of personal information such as location and personal preferences. Thus, privacy-related interactions between service providers and end users are important to be studied as personal data are valuable in a subscription-based cloud system. In our research, a game theory approach is used as a tool to identify and analyse such interactions to understand stakeholder choices, as well as how to improve the quality of the service offered in a cloud computing setting.

We have argued that it is very important to take security and privacy into account when designing and using cloud services. In this work security in cloud computing was elaborated in a way that covers security issues and challenges, security standards and security management models. Security standards offer some kind of security template which cloud service providers (CSP) could obey. Security management models offer recommendations based on security standards and best practices. These are all very important topics which will be certainly discussed in the upcoming years of cloud computing.
In this work we examined provider’s compliance with its public security policy and undeclared secondary usage of data. In this work we focused on the effectiveness of data protection and we leave deliberate violation of security policy out of scope.

A way to resolve the issue of asymmetric information is to engage third party assurance. This usually implies a certification scheme. In the case of information security ISO provides such a scheme based on the ISO/IEC 27001 standard (ISO, 2013). ISO/IEC 27001 specifies the requirements for Information Security Management Systems. Companies can be certified against ISO27001 by one of the accredited bodies.

The aim of this work is to examine how asymmetric information on the security system implemented by the CSP affects the strategic choices of CSPs and consumers. Moreover, we examine the role of security certification and how it may change the strategic choices of consumers and CSPs.

With regard to the payoffs, consumer would have a benefit of B if he/she purchases cloud services from a provider that implements an effective ISMS. Otherwise, if the CSP does not provide adequate security then consumer’s payoff is reduced by L, i.e. the loss resulting from a security breach. In this basic model we assume that a security breach will certainly happen if there is no adequate security in place. This assumption is removed in subsequent enhanced models. If the consumer does not buy, then the payoff is equal to zero, meaning that he/she doesn’t lose or earn anything. From the CSPs side, profit P is reduced by the cost of implementing and maintaining an effective ISMS, which is marked as C. If the CSP implements ISMS and the consumer doesn’t buy, then the CSP has a loss that equals C. If the CSP doesn’t implement ISMS, it gets a profit of P when the consumer buys and a profit of zero when the consumer doesn’t buy.

If the CSP and the consumer interact only once, then they are playing a single stage game. In the stage game if B ≥ L the strategic profile (No ISMS, Buy) constitutes the only Nash Equilibrium. Otherwise, if B < L then (No ISMS, Don’t Buy) is an equilibrium. In other words, if the consumer values the benefits of cloud services as more important than the loss in case of a security breach, then he/she will purchase the services. There is no Nash Equilibrium in the stage game in which the CSP implements an effective ISMS. Consequently, all potential users of cloud services that have sensitive data are deterred from purchasing cloud services. This result is in line with the characterisation of security as a lemons market.

In most cases a CSP would aim for a long-term relationship with customers. In this case, the CSP-Consumer interaction is modelled as an infinitely repeated game. In this case, the term infinitely repeated game refers to a game that is repeated for an undefined period of time. In the repeated game, consumers have to make a choice whether to renew their subscription. This is equivalent to a new purchase of cloud services. Players in repeated games can follow
complex strategies, which may depend on what the other player played in the previous periods. According to the “folk theorem” for repeated games if the players are sufficiently patient, then any feasible, individually rational payoff vector of the stage game constitutes a sub-game perfect equilibrium payoff in the associated infinitely repeated game.
6. Conclusions

6.1. Summary of research results and discussion

E-government initiatives focus, to a great extends, on technology-related factors. We argue that e-government technology designers and policy-makers should also consider social and cultural factors. We believe that there is much to benefit from the social theory perspective. In this research we focused on intention to use. It would be most interesting for future research to examine the degree to which intention of use would lead to actual use. If not, it would be useful to study the factors that have deterred them from their initial perception.

The effect of cultural bias is mostly neglected by policy makers. They focus on showing that e-government technologies are useful and easy to use and they attempt to downplay privacy concerns. These are important issues, especially the privacy issue. Nevertheless, often they fail to address the mindset of specific cultural groups that object these technologies. Egalitarians would not be easily persuaded that there are no risks for their privacy. However, they might set aside those concerns, if they come to believe that these new technologies would fight social inequalities and benefit a large group of people. Fatalists, on the other hand, are indifferent, in the sense that they would not make any effort to reach new technologies, but they would use it if they are “handed” to them.

However, our analysis was limited to the Greek region and only to one specific e-government initiative, the Tax Card. It would be of a high interest to conduct similar surveys to other world-wide cases. In the following paragraphs we shall attempt to interpret the results of the game theoretic analysis and discuss possible remedies. The preceding analysis shows why it is difficult to establish trust with regard to the use of personal information in electronic commerce. Any e-shop that does not consider retaining its customers for a long period to be a desirable or attainable aim would choose to exploit the personal information of its customers in order to maximize its profit.

Thus, in an internet market where customers move from shop to shop without any migration cost and without any benefit from remaining loyal to a particular e-shop privacy policies can not establish trust. E-shops would not invest in establishing and maintaining a strict privacy policy. Since, consumers don’t know in advance which e-shop is reliable and which is not, they will employ some privacy protection technique. In most cases they would fake their personal information.

On the contrary, e-shops targeting consumers that would make regular buys and remain loyal if satisfied would refrain from mistreating personal information of their customers. However, this holds only for observable policy violations. If privacy policy violations have a low probability to get detected, then the privacy-sensitive consumer would assume that the e-
shop will mistreat his/her personal information and, thus, he/she will employ some method of privacy protection.

Thus, since voluntary privacy policies and relevant technologies, such as P3P and Privacy Agents, are not able to establish trust between sellers and buyers, we should seek for remedies. Our analysis shows that any remedy should either address consumer loyalty or impose a penalty to violating sellers. Some options are:

• Regulate the use of policies by enforcing audits. However, one should consider the cost of audits and the possible low effectiveness, since such violations are notoriously difficult to detect.

• Impose high penalties for violating e-shops. However, this will only be effective if there is a reasonable detection rate.

• Establishing reputation systems. This is an effective strategy in several cases. If privacy violating sellers expect to lose massively potential buyers, then they might not risk mistreating the personal information of their customers.

In any case, the above conclusions only apply to privacy-sensitive buyers. We should not disregard the fact that a large part of the population is not willing to put much effort in protecting their privacy, either because they feel that the information they reveal is not very sensitive, or because they feel that in the Internet world there is no effective way to protect your privacy.

In the following paragraphs we will present some preliminary results from the above game model. Where end users have the ability to choose a cloud service provider to match their expectations, their stated privacy policies cannot assure trust. The utilization of cloud computing services, such as in the content delivery domain is growing, however, it is still extremely difficult for many end users to trust service providers and store their personal data in a cloud-based environment, as privacy violation issues may perceivably happen at any time. When end users adopt cloud-based services and chose to use relevant apps, they do not know in advance, if the service provider is reliable with respect to retention of their personal data. There are many instances where end users provide fake personal information in order to receive services (e.g. cloud-based storage) as they feel more protected. On the other hand, service providers are interested to implement their strategic policies so that end users would remain loyal and pay for premium services. In this case, they should carefully consider giving data to a third party in order to avoid disappointing both their premium and basic end users and salvage their reputation. Providing a fair solution to assure both end users’ loyalty and SP compliance is required. However, since such violations are difficult to be detected by most stakeholders, regulating the use of policies by enforcing audits is rather of low effectiveness. Enforcing penalties for any violation from SPs or using reputation systems are helpful
countermeasures that provide assurance to end-users. SPs might not risk illicitly offending personal data, when they are expected to lose a number of potential end users from such practices. To summarize, we note that the above findings are applicable only to end users that care about privacy policies and are sensitive to privacy violations. Other end users may not behave in the same way, either because they believe that Internet users in general cannot protect their privacy in an effective way, or because they believe that the information they reveal is not useful for further use by the SP or other third parties.

6.2. Implications to Theory

E-commerce transactions, in addition to the exchange of goods and services for payment, often entail an indirect transaction, where personal data are exchanged for better services or lower prices. This paper analyses buyer’s and seller’s privacy-related strategic choices in e-commerce transactions through game theory. We demonstrate how game theory can explain why buyers mistrust internet privacy policies and relevant technologies (e.g. P3P) and sellers hesitate to invest in data protection.

To summarize, we note that the above findings are applicable only to end users that care about privacy policies and are sensitive to privacy violations. Other end users may not behave in the same way, either because they believe that Internet users in general cannot protect their privacy in an effective way, or because they believe that the information they reveal is not useful for further use by the SP or other third parties.

6.3. Implications to Practice

On the contrary, e-shops targeting consumers that would make regular buys and remain loyal if satisfied would refrain from mistreating personal information of their customers. However, this holds only for observable policy violations. If privacy policy violations have a low probability to get detected, then the privacy-sensitive consumer would assume that the e-shop will mistreat his/her personal information and, thus, he/she will employ some method of privacy protection.

Thus, since voluntary privacy policies and relevant technologies, such as P3P and Privacy Agents, are not able to establish trust between sellers and buyers, we should seek for remedies. Our analysis shows that any remedy should either address consumer loyalty or impose a penalty to violating sellers. Some options are:

• Regulate the use of policies by enforcing audits. However, one should consider the cost of audits and the possible low effectiveness, since such violations are notoriously difficult to detect.

• Impose high penalties for violating e-shops. However, this will only be effective if there is a reasonable detection rate.
• Establishing reputation systems. This is an effective strategy in several cases. If privacy violating sellers expect to lose massively potential buyers, then they might not risk mistreating the personal information of their customers.

6.4. Limitations and Future Research

It was shown that although it would be more profitable for sellers and buyers to be honest to each other and cooperate, the buyer-seller game will end in an equilibrium where the seller does not abide to the privacy policy and the buyer provides fake information. As a result, internet privacy policies are disregarded by consumers. We have also shown that in order for privacy policies to have an impact on consumer they should be accompanied by regulations that impose a high penalty for violating sellers or reputation systems that increase the cost of violation. Nevertheless, this study has several limitations as some potentially significant factors have been excluded. Specifically we have excluded the factor of discount of future benefits, which is a common factor in infinitely repeated games. We have only considered the game between a buyer and a seller and we have not analyzed the case of many buyers that communicate with each other and exchange information about the trustworthiness of sellers. Finally, we have not considered consumers that are not privacy sensitive. In this paper we have not presented the formal definition and analysis of our game model, so as to make it readable for a wider audience. Formal definition and analysis is left for future research.

E-government initiatives often face citizens’ mistrust, particularly when they involve the collection and processing of personal data. In this paper we present the results of an empirical study regarding citizens’ intention to use a new service offered by the Greek Ministry of Finance, the so called “Tax Card”. Tax Card is used to collect information about everyday purchases and aims to diminish tax avoidance. We have examined the strong influence of Cultural Bias on the formulation of citizens’ intention to use and concluded that different cultural types of people should be addressed in different ways in order to achieve broad adoption of e-government services.

The effect of cultural bias is mostly neglected by policy makers. They focus on showing that e-government technologies are useful and easy to use and they attempt to downplay privacy concerns. These are important issues, especially the privacy issue. Nevertheless, often they fail to address the mindset of specific cultural groups that object these technologies. Egalitarians would not be easily persuaded that there are no risks for their privacy. However, they might set aside those concerns, if they come to believe that these new technologies would fight social inequalities and benefit a large group of people. Fatalists, on the other hand, are indifferent, in the sense that they would not make any effort to reach new technologies, but they would use it if they are “handed” to them.
E-government initiatives focus, to a great extent, on technology-related factors. We argue that e-government technology designers and policy-makers should also consider social and cultural factors. We believe that there is much to benefit from the social theory perspective.

In this research we focused on intention to use. It would be most interesting for future research to examine the degree to which intention of use would lead to actual use. If not, it would be useful to study the factors that have deterred them from their initial perception. However, our analysis was limited to the Greek region and only to one specific e-government initiative, the Tax Card. It would be of a high interest to conduct similar surveys to other world-wide cases.
References

Ackerman, M., Darrell, T., Weitzner, D.: Privacy in Context. Human Computer Interaction 16(2), 167–176 (2001)

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the ACM Conference on Electronic Commerce (EC 2004), pp. 21–29.

Acquisti, A. and J. Grossklags (2007). What can behavioral economics teach us about privacy? In S. G. C. L. Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), Digital Privacy: Theory, Technologies and Practices, pp. 363–377. Auerbach Publications (Taylor and Francis Group).

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26–33.

Acquisti, A. and H. R. Varian (2005). Conditioning prices on purchase history. Marketing Science 24 (3), 367–381.

Acquisti, A. (2010). The economics of personal data and the economics of privacy. Background Paper for OECD Joint WPISP-WPIE Roundtable.

Acquisti, A. (2010). From the economics to the behavioral economics of privacy: A note. In Ethics and Policy of Biometrics (pp. 23-26). Springer, Berlin, Heidelberg.

Acquisti, A., L. K. John, and G. Loewenstein (2013). What is privacy worth? The Journal of Legal Studies, Vol.42, No. 2, pp.249-274

Acquisti, A. (2013). The economics of privacy: Theoretical and empirical aspects. Nova.

Acquisti, A. (2014). From the economics of privacy to the economics of big data.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442-92.

Adams, D. A., Nelson, R. R. and Todd, P. A. (1992) ‘Perceived usefulness, ease of use, and usage of information: A replication’, MIS Quarterly, Vol. 16, No. 2, pp.227-247.

A. Adams, C., Muir, S., & Hoque, Z. (2014). Measurement of sustainability performance in the public sector. Sustainability Accounting, Management and Policy Journal, 5(1), 46-67.

Adams, J. (2016). Risk and culture. Routledge Handbook of Risk Studies, p.83.
Adjerid, I., Peer, E., & Acquisti, A. (2016). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. Available at SSRN 2765097.

Agarwal R, Karahanna E (2000) Time flies when you’re having fun: Cognitive absorption and beliefs about information technology usage. MIS Quart, Vol.24, No.4, pp.665–692.

Aguirre, E., Roggeveen, A. L., Grewal, D., and Wetzels, M. (2016). The personalization-privacy paradox: implications for new media. Journal of Consumer Marketing, Vol.33, No.2, pp.98-110.

Aiimeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. Computers in Human Behavior, 58, 368-379.

Alenezi, H., Tarhini, A. and Masa’deh, R. (2015). “Investigating the strategic relationship between information quality and e-government benefits: a literature review”, International Review of Social Sciences and Humanities, Vol. 9 No. 1, pp. 33-50.

Al-Somali, S. A., Gholami, R., & Clegg, B. (2009). An investigation into the acceptance of online banking in Saudi Arabia. Technovation, 29(2), 130-141.

Almarabeh, T. And AbuAli, A. (2010), "A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success", European Journal of Scientific Research, Vol.39, No.1, pp. 29-42.

Alzahrani, L., Al-Karaghouli, W., and Weerakkody, V. (2016). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. International Business Review.

Anastasopoulou, K., Tryfonas, T. and Kokolakis, S. (2013) Strategic interaction analysis of privacy-sensitive end-users of cloud-based mobile apps, in L. Marinos and I. Askoxylakis (eds), Human aspects of information security, privacy, and trust, Springer LNCS 8030, Springer-Verlag Berlin Heidelberg 2013.

Angst CM, Agarwal R (2009) Adoption of electronic health recordsin the presence of privacy concerns: The elaboration likelihood model and individual persuasion. MIS Quarterly, Vol.33, No.2, pp.339–370.

Anton, A. I., Earp, J. B., Young, J. D. (2010), “How Internet users’ privacy concerns have evolved since 2002”,IEEE Security and Privacy, Vol. 8, No. 1, pp. 21–27.

Ardagna, D., Panicucci, B., & Passacantando, M. (2011, March). A game theoretic formulation of the service provisioning problem in cloud systems. In Proceedings of the 20th international conference on World wide web (pp. 177-186). ACM.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.
Arnott, D. (2006). Cognitive biases and decision support systems development: A design science approach. Information Systems Journal, Vol.16, pp.55-78

Backes, M., Bugiel, S., Hammer, C., Schranz, O., & von Styp-Rekowsky, P. (2015, August). Boxify: Full-fledged App Sandboxing for Stock Android. In USENIX Security Symposium (pp. 691-706).

Bagozzi, R.P., Davis, F.D. and Warshaw, P.R. (1992), “Development and test of a theory of technological learning and usage”, Human Relations, Vol. 45 No. 7, pp. 660-686.

Bansal G, Zahedi FM, Gefen D (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems Vol.49, No.2, pp.138–150.

Bansal, G., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. European Journal of Information Systems, 24(6), 624-644.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information & Management, 53(1), 1-21.

Bauer, R. A. (1960) ‘Consumer behavior as risk-taking’ in Hancock, R. S. (Eds): Dynamic marketing for a changing world, pp.389-398.

Bazerman, M. H., and Moore, D. A. (2009). Judgment in managerial decision making (7th Ed.). New York: Wiley and Sons.

Beatty, P., Reay, I., Dick, S. and Miller. J. (2007). “P3P Adoption on E-Commerce Web sites: A Survey and Analysis”, IEEE Internet Computing, vol. 11, pp. 65-71.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. Physical review letters, 68(21), 3121.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS quarterly, 35(4), 1017-1042.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. Communications of the ACM, 48(4), 101-106.

Berkelaar, B. L. (2014). Cybervetting, online information, and personnel selection: New transparency expectations and the emergence of a digital social contract. Management Communication Quarterly, 28(4), 479-506.

Benitez, K., & Malin, B. (2010). Evaluating re-identification risks with respect to the HIPAA privacy rule. Journal of the American Medical Informatics Association, 17(2), 169-177.
Bevir, M., Rhodes, R. A., & Weller, P. (2003). Traditions of governance: interpreting the changing role of the public sector. *Public administration, 81*(1), 1-17.

Bijker, W. E., Hughes, T. P., Pinch, T., & Douglas, D. G. (2012). *The social construction of technological systems: New directions in the sociology and history of technology*. MIT press.

Blackmer, W. S. (2016). GDPR: Getting Ready for the New EU General Data Protection Regulation. *Information Law Group, InfoLawGroup LLP, Retrieved, 22*(08), 2016.

Blumenthal-Barby, J. S., & Krieger, H. (2015). Cognitive biases and heuristics in medical decision making: a critical review using a systematic search strategy. *Medical Decision Making, 35*(4), 539-557.

Bomil, S. and Ingoo H. (2003), “The IS risk analysis based on a business model”, Journal Information and Management, Vol. 41 No. 2, p.p 149 – 158.

Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research, 5*(1), 62-70.

Brunette, G. and R. Mogull (ed). 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, December 2009.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347.

Brey, P. A. (2012). Anticipatory ethics for emerging technologies. *NanoEthics, 6*(1), 1-13.

Bosse, D. A., & Phillips, R. A. (2016). Agency theory and bounded self-interest. Academy of Management Review, *41*(2), 276-297

Browne, G. J. and Parson, J. 2012.More Enduring Questions in Cognitive IS Research, Journal of the Association for Information Systems Vol. 13, Issue 12, pp. 1000-1011.

Browne, G. J., & Ramesh, V. (2002). Improving information requirements determination: a cognitive perspective. *Information & Management, 39*(8), 625-645.

Buchanan T, Paine C, Joinson AN, Reips U (2007) Development of measures of online privacy concern and protection for use on the internet. J. Amer. Soc. Inform. Sci. Tech. Vol.58, No.2, pp.157–165.

Buyya, R., C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic (2009) “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility,” Future Generation Computer Systems (25)6, pp. 599–616.

Cai, C. X., Mei, S. E., & Zhong, W. J. (2016). A game-theory approach to manage decision errors. In MATEC Web of Conferences (Vol. 44). EDP Sciences.
Calheiros, R. N. Ranjan, R. Rose, C. A. F. D. and Buyya, R. “CloudSim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services,” CoRR, vol.abs/0903.2525, 2009.

Camerer, C.F. (2003). Behavioral Game Theory: Experiments on Strategic Interaction. Princeton, NJ:Princeton University Press.

Camerer, C. F., Loewenstein, G., & Prelec, D. (2004). Neuroeconomics: Why economics needs brains. The Scandinavian Journal of Economics, 106(3), 555-579.

Camerer, C. F. (2011). Behavioral game theory: Experiments in strategic interaction. Princeton University Press.

Camp, L. J. 2003. Design for trust. In Trust, Reputation and Security: Theories and Practice, Rino Falcone, editor. Springer-Verlang, 2003

Camp, L. J. (1999). Web security and privacy: An American perspective. The Information Society, Vol.15 No.4, pp. 249-256.

Capling, A., & Ravenhill, J. (2011). Multilateralising regionalism: what role for the Trans-Pacific Partnership Agreement?. The Pacific Review, 24(5), 553-575.

Carbajal, J. C., & Ely, J. C. (2016). A model of price discrimination under loss aversion and state-contingent reference points. Theoretical Economics, 11(2), 455-485.

Carey, R., & Burkell, J. (2009). A heuristics approach to understanding privacy-protecting behaviors in digital social environments. Lessons from the identity trail, 65-82.

Casalino, N. (2014), “Learning to connect: a training model for public sector on advanced e-government services and inter-organizational cooperation”, International Journal of Advanced Corporate Learning (iJAC), Vol. 7 No. 1, pp. 24-31.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. Journal of Management Information Systems, 25(2), pp.281-304.

Cazier, J. A., Jensen, A. S., and Dave, D. S. (2008) ‘The Impact of Consumer Perceptions of Information Privacy and Security Risks on the Adoption of Residual RFID Technologies’, Communications of the Association for Information Systems, Vol. 23, No. 1, pp.235-256.

Cellini, S. R., & Kee, J. E. (2010). Cost-effectiveness and cost-benefit analysis. Handbook of practical program evaluation, 3

Chaiken, S., Wood, W., & Eagly, A. H. (1996). Principles of persuasion.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer’s dilemma. Information technology and management, 6(2-3), 181-202.
Christozov, D., Chukova, S., & Mateev, P. (2009). Informing processes, risks, evaluation of the risk of misinforming. Foundations of informing science, pp. 323-356.

Clarke, R., 2009, “Privacy impact assessment: Its origins and development”, Computer law and security review, Vol.25, No.2, pp. 123–135.

Conner, W., Iyengar, A., Mikalsen, T., Rouvellou, I., Nahrstedt, K.: A Trust Management Framework for Service-Oriented Environments. In: Proc. of WWW 2009, Madrid, Spain.

Council, I. A. (2012). Federal risk and authorization management program (FedRAMP).

Cranor, L.F. (2003)"P3P: Making privacy policies more useful", IEEE Security and Privacy, vol. 1, no. 6, pp. 50-55.

Cranor, L.F., Gudure, P. and Arjula, M. (2006). “User interfaces for privacy agents”, ACM Transactions on Computer-Human Interaction (TOCHI), vol. 13, pp. 135-178.

Creech, K. C. (2013). Electronic media law and regulation. Routledge.

CTIA (2008) Best practices and guidelines for location based services. The Cellular Telecommunications and Internet Association (CTIA). http://www.ctia.org/content/index.cfm/AID/1130

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science, 10(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. Journal of social issues, 59(2), 323-342.

Dake, K. (1991) ‘Orienting Dispositions in the Perception of Risk: An Analysis of Contemporary Worldviews and Cultural Biases’, Journal of Cross-Cultural Psychology, Vol. 22, No. 1, pp.61-82.

Dempsey, M. (2015). Stock Markets, Investments and Corporate Behavior: A Conceptual Framework of Understanding. World Scientific.

Davis, F. D., Bagozzi, R. P. and Warshaw, P. R. (1989) ‘User Acceptance of Computer Technology: A Comparison of Two Theoretical Models’, Management Science, Vol. 35, No. 8, pp. 982-1003.

Davis, F.D. (1989), “Perceived usefulness, perceived ease of use, and user acceptance of information technology”, MIS Quarterly, Vol. 13 No. 3, pp. 319-339.

Doelitzscher, F., Sulistio, A., Reich, C., Kuijs, H. and Wolf, D. Private cloud for collaboration and e-learning services: from IaaS to SaaS, Computer 91 (2011) 23–42.

Douglas, M. and Wildavsky, A. (1982) Risk and Culture: An Essay on Selection of Technological and Environmental Dangers, California University Press, Berkeley.
De Hert, P., Papakonstantinou, V., & Kamara, I. (2016). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. Computer Law & Security Review, 32(1), 16-30.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80.

Directive 95/ /EC of the european parliament and the council of the european union. Chapten II. General rules on the lawfulness of the processing of personal data (n.d.). Retrieved from https://aspe.hhs.gov/report/directive-95-ec-european-parliament-and-council-euro

Dopfer, K., & Potts, J. (2015). The general theory of economic evolution. Routledge.

Douss, A. B. C., Abassi, R., & El Fatmi, S. G. (2014, September). A Trust Management Based Security Mechanism against Collusion Attacks in a MANET Environment. In Availability, Reliability and Security (ARES), 2014 Ninth International Conference on (pp. 325-332). IEEE.

Drexler, W., & Fujimoto, J. G. (2015). Optical coherence tomography: technology and applications. Springer.

Edelman B (2011) Adverse selection in online “trust” certifications and search results. Electronic Commerce Res. Appl. Vol.10, No.1, pp.7–25

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. Academy of management review, 14(1), 57-74.

Einstein, A., 1965. Concerning an heuristic point of view toward the emission and transformation of light. American Journal of Physics, 33(5), p.367.

European Network and Information Security Agency – ENISA (2009). Cloud Computing: Benefits, Risks and Recommendations for Information Security. Available at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (accessed 14/07/2016).

Evans, J. S. B. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. Annu. Rev. Psychol., 59, 255-278.

Evans, J. S. B., & Stanovich, K. E. (2013). Dual-process theories of higher cognition: Advancing the debate. Perspectives on psychological science, 8(3), 223-241.

Fagnani, F., Franci, B., & Grasso, E. (2016). A game theoretic approach to a peer-to-peer cloud storage model. arXiv preprint arXiv:1607.02371

Falk, A. (2007). Gift exchange in the field. Econometrica, 75(5), 1501-1511.Farrell, J. (2012). The economics of privacy: Can privacy be just another good? J. onTelecomm. and High Tech. L., Vol.10, pp.251-445.
Farrell, J. (2012). The economics of privacy: Can privacy be just another good? J. on Telecomm. & High Tech. L. 10, 251-445.

Featherman, M. S. and Pavlou, P. A. (2003) ‘Predicting E-Services Adoption: A Perceived Risk Facets Perspective’, International Journal of Human-Computer Studies, Vol. 59, No.4, pp.451-474.

Fehr, E., & Schmidt, K. M. (1999). A theory of fairness, competition, and cooperation. The quarterly journal of economics, 114(3), 817-868.

Friedman E.J. and Resnick, P. “The Social Cost of Cheap Pseudonyms”, Journal of Economics and Management Strategy, Vol. 10, No. 2, 2001, pp. 173-199.

Fudenberg, D. (2006). Advancing beyond advances in behavioral economics. Journal of Economic Literature, 44(3), 694-711.

Gal-Oz, N., Grinshpoun, T., & Gudes, E. (2011). Privacy issues with sharing reputation across virtual communities. In Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society (p. 3). ACM.

Gao, X., & Zhong, W. (2016). A differential game approach to security investment and information sharing in a competitive environment. IIE Transactions, 48(6), 511-526.

Gawronski B, Bodenhausen GV. Associative and propositional processes in evaluation: an integrative review of implicit and explicit attitude change. PsycholBull2006, Vol. 132, pp.692–731.

Gellman, R. (2016). Fair information practices: A basic history. Browser Download This Paper.

Geman, D., & Reynolds, G. (1992). Constrained restoration and the recovery of discontinuities. IEEE Transactions on pattern analysis and machine intelligence, 14(3), 367-383.

Ghose, R. (2005). The complexities of citizen participation through collaborative governance. Space and Polity, 9(1), 61-75.

Ghose, R., & Pettygrove, M. (2014). Urban community gardens as spaces of citizenship. Antipode, 46(4), 1092-1112.

Gigerenzer, G., Todd, P. M., and the ABC Research Group. (1999). Simple heuristics that make us smart. Oxford: Oxford University Press

Gigerenzer, G. (1991). How to make cognitive illusions disappear: Beyond “heuristics and biases”. European review of social psychology, 2(1), 83-115.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. Annual review of psychology, 62, 451-482.
Gilhooly, K. J., & Fioratou, E. (2009). Executive functions in insight versus non-insight problem solving: An individual differences approach. *Thinking & Reasoning, 15*(4), 355-376.

Gintis, H. (2014). *The bounds of reason: Game theory and the unification of the behavioral sciences*. Princeton University Press.

Grendstad, G. (2000) ‘Grid-Group Theory and Political Orientations: Effects of Cultural Biases in Norway in the 1990s’, Scandinavian Political Studies, Vol.23, No. 3, pp. 217-244.

Grossklags, J., & Acquisti, A. (2007, June). When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In *WEIS*.

Gutwirth, S., & Hert, P. (2008). Regulating profiling in a democratic constitutional state. *Profiling the European citizen*, 271-302.

Hagman, W. (2013). Affective Biases and Heuristics in Decision Making: Emotion regulation as a factor for decision making competence.

Halachmi, A., & Greiling, D. (2013). Transparency, e-government, and accountability: Some issues and considerations. *Public Performance & Management Review, 36*(4), 562-584.

Han, Y. (2010). On the clouds: A new way of computing. *Information Technology & Libraries, 29*(2), 87-92.

Hann, I-H., Hui, K-L., Lee, T.S., and Png, I.P.L., 2002. The Value of Online Information Privacy: Evidence from the USA and Singapore. International Conference on Information Systems.

Hann, I. H., Hui, K. L., Lee, T., and Png, I. 2007. Overcoming Information Privacy Concerns: An Information Processing Theory Approach. *Journal of Management Information Systems, Vol.24*, No.2, pp. 13-4

Haselton, M. G., Nettle, D., & Murray, D. R. (2005). The evolution of cognitive bias. *The handbook of evolutionary psychology*.

Hausken K. 2002. Probabilistic risk analysis and game theory. *Risk Analysis*, vol. 22, pp. 17–27.

Heine, S. J. (2008), Cultural psychology, W.W. Norton, New York.

Heijden, H., Verhagen, T., and Creemers, M. (2003) ‘Understanding Online Purchase Intentions: Contributions from Technology and Trust Perspectives’, *European Journal of Information Systems, Vol. 12*, No. 1, pp.41-48.

Heine, S. J. (2008), Cultural psychology, W.W. Norton, New York.

Hendrickson, A.R., Massey, P.D. and Cronan, T.P. (1993) 'On the test-retest reliability of perceived usefulness and perceived ease of use scales', *MIS Quarterly, Vol. 17*, No. 2, pp.227-230.
Hernandez, R. T. (1988). ECPA and online computer privacy. *Fed. Comm. LJ*, 41, 17.

Hilty, L. M., & Aebischer, B. (2015). Ict for sustainability: An emerging research field. In *ICT Innovations for Sustainability* (pp. 3-36). Springer, Cham.

Hirshleifer, J. (1980). Privacy: Its origin, function, and future. *The Journal of Legal Studies*, 9(4), 649-664.

Hirshleifer, D. A., Huang, C., & Teoh, S. H. (2016). Information Asymmetry, Market Participation, and Asset Prices. Market Participation, and Asset Prices.

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications*, 9(1), 50-60.

Hofstede, G. (1980) *Culture’s Consequences: International Differences in Work-Related Values*, Sage, Beverly Hills, CA.

Hofstede, G. (2001). *Culture’s Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*. Thousand Oaks, CA: Sage (co-published in the PRC as Vol. 10 in the Shanghai Foreign Language Education Press SFLEP Intercultural Communication Reference Series, 2008).

Hui, K.-L., Teo, H.-H., Lee, S.-Y. T. 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, Vol.31, No.1, pp.19-33.

Humberg, T. and Jürjens, J. (2016) Compliance in Clouds. *Encyclopedia of Cloud Computing*, 267-273.

Humphreys, E. (2011). Information security management system standards. Datenschutz und Datensicherheit-DuD, vol.35(art.1), pp.7-11.

Hwang, K., Li, D.: Trusted Cloud Computing with Secure Resources and Data Coloring. *IEEE Internet Computing* 14(5), 14–22 (2010)

IRM (2002) A Risk Management Standard, Institute of Risk Management, London, UK, Available at: [https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf](https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf)

Irvin, R. A., & Stansbury, J. (2004). Citizen participation in decision making: is it worth the effort?. *Public administration review*, 64(1), 55-65.

ISO/IEC 27001-2013: Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, Switzerland, 2013.

Jansen, A. (2005) ‘Assessing e-government progress– why and what’, Proc. NOKOBIT 2005, 21-23 November, Bergen, Norway.
Janson, A., Hoffmann, A., Hoffmann, H., & Leimeister, J. (2014). How Customers Trust Mobile Marketing Applications.

Janssen, M., & van den Hoven, J. (2015). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?

Jebalia, M., Ben Letaïfa, A., Hamdi, M., & Tabbane, S. (2015). An overview on coalitional game-theoretic approaches for resource allocation in cloud computing architectures. International Journal of Cloud Computing 22, 4(1), 63-77.

Jensen, S. (2013). Abusing the Computer Fraud and Abuse Act: Why broad interpretations of the CFAA fail. Hamline L. Rev., 36, 81.

Jhang-Li, J.H. and Chiang, I.R. 2015. Resource allocation and revenue optimization for cloud service providers, Decision Support Systems 77 pp.55–66.

Joshi, S. Sun, Y.A. and Vora, P.(2006) Randomization as a strategy for sellers during price discrimination, and impact on bidders' privacy, Proceedings of the 5th ACM workshop on Privacy in electronic society, October 30-30, Alexandria, Virginia, USA.

Figliola, P. M., & Fischer, E. A. (2015). Overview and issues for implementation of the federal cloud computing initiative: Implications for federal information technology reform management. US Congressional Research Service (CRS), 1.

Friedman, E.J. and Resnick, P.(2001). “The Social Cost of Cheap Pseudonyms”, Journal of Economics and Management Strategy, vol. 10, no. 2, pp. 173-199.

Frydman, C., & Camerer, C. F. (2016). The psychology and neuroscience of financial decision making. Trends in cognitive sciences, 20(9), 661-675.

Kahneman, D. (2003). A perspective on judgment and choice: mapping bounded rationality. American psychologist, 58(9), 697.

Kahneman, D., & Tversky, A. (2013). Choices, values, and frames. In HANDBOOK OF THE FUNDAMENTALS OF FINANCIAL DECISION MAKING: Part I (pp. 269-278).

Kahneman, D. (2011). Thinking, fast and slow. New York: Farrar, Strous and Giroux

Kahneman D. and Tversky A., Choices, Values, and Frames, Cambridge Univ. Press, 2000.

Kahneman, D. & Tversky, A. (1974).“Judgment under Uncertainty: Heuristics and Biases,” Science185, pp. 1124–1131.

Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk. In Handbook of the fundamentals of financial decision making: Part I (pp. 99-127).

Kang, J., Shilton, K., Estrin, D., Burke, J. and Hansen, M. (2010).“Self-Surveillance Privacy” Iowa Law Review, Vol. 97, p. 809, 2012; UCLA School of Law Research Paper No. 11-01.
Kash, I. A., & Key, P. B. (2016). Pricing the Cloud. IEEE Internet Computing, 20(1), 36-43.

Katzan Jr., H. (2010c). “On the Privacy of Cloud Computing,” International Journal of Management and Information Systems (14)2, p. 1.

Kaur, P. D., & Chana, I. (2014). A resource elasticity framework for QoS-aware execution of cloud applications. Future Generation Computer Systems, 37, 14-25.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal, 25(6), 607-635.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision support systems, 44(2), 544-564.

Kim, W. (2011). Cloud computing adoption. International Journal of Web and Grid Services, 7(3), 225-245.

Kim, S., & Lee, J. (2012). E-participation, transparency, and trust in local government. Public Administration Review, 72(6), 819-828.

King, N.J. and Raja, V.T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, pp.308-319.

Klabunde, A., & Willekens, F. (2016). Decision-making in agent-based models of migration: state of the art and challenges. European Journal of Population, 32(1), 73-97.

Krishnamurthy, B., & Wills, C. E. (2009, August). On the leakage of personally identifiable information via online social networks. In Proceedings of the 2nd ACM workshop on Online social networks (pp. 7-12). ACM.

Kokolakis, S., Anastasopoulou, K. Karyda, M. “An Analysis of Privacy-related Strategic Choices of Buyers and Sellers in e-Commerce Transactions”, in Proc. of the 16th Panhellenic Conference on Informatics with international participation, Pireaus, Greece - October 5-7, 2012.

Kube, S., Maréchal, M. A., & Puppe, C. (2012). The currency of reciprocity: Gift exchange in the workplace. American Economic Review, 102(4), 1644-62.

Lauber, T. B., & Knuth, B. A. (2000). Citizen participation in natural resource management: a synthesis of HDRU research.
Lawton, G. (2008a) “Developing Software Online With Platform-as-a-Service Technology,” Computer (41)6, pp. 13–15.

Leavitt, N. (2009) “Is Cloud Computing Really Ready for Prime Time?” Computer (42)1, pp. 15–20.

Lee, James Jr.; Warkentin, Merrill; and Johnston, Allen C. (2016) "A Broader View of Perceived Risk during Internet Transactions," Communications of the Association for Information Systems : Vol. 38, Article 8.

Li, W., and Huang, Z. (2016). The Research of Influence Factors of Online Behavioral Advertising Avoidance. American Journal of Industrial and Business Management, 6(09), 947.

Li, K., Liu, C., Li, K., & Zomaya, A. (2015). A framework of price bidding configurations for resource usage in cloud computing.

Liang, H., Shen, F., and Fu, K. W. (2016). Privacy protection and self-disclosure across societies: A study of global Twitter users. Available at New Media and Society, 146144816642210.

Lian, J. W., Yen, D. C., & Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. International Journal of Information Management, 34(1), p.p.28-36.

Lilien, L., & Bhargava, B. (2008). Trading privacy for trust in online interactions. Idea Group.

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. Industrial Management & Data Systems, 111(7), p.p.1006-1023.

Lumer, C. (2010). Moral desirability and rational decision. Ethical theory and moral practice, 13(5), 561-584.

Maghrabi, L., & Pfluegel, E. (2015). Moving assets to the cloud: A game theoretic approach based on trust. In Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on (pp. 1-5). IEEE.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (UIIPC): The construct, the scale, and a causal model. Information systems research, 15(4), 336-355.

Mamadouh, V. (1999) "Grid-group cultural theory: an introduction", GeoJournal, 1999, vol. 47, No. 3, pp. 395-409.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. Journal of social issues, 59(2), 243-261.
McCluskey, J. (2000). A game theoretic approach to organic foods: An analysis of asymmetric information and policy. Agricultural and Resource Economics Review, 29(1), pp.1-9.

McKnight, D.H., Choudhury, V. and Kacmar, C., (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building mode. Journal of Strategic Information Systems 11(3-4), pp.297–323.

McKinney Jr, E. H., & Yoos, C. J. (2010). Information about information: A taxonomy of views. MIS quarterly, pp.329-344.

Mei, J., Li, K., Ouyang, A., & Li, K. (2015). A profit maximization scheme with guaranteed quality of service in cloud computing. IEEE Transactions on Computers, 64(11), 3064-3078.

Mell, P., & Grance, T. (2009). Effectively and securely using the cloud computing paradigm. NIST, Information Technology Laboratory, 304-311.

Mell, P., and T. Grance (2010) “The NIST Definition of Cloud Computing,” Communications of the ACM (53)6, p. 50.

Morgan, L., & Conboy, K. (2013). Key factors impacting cloud computing adoption. Computer, 10,97999

Morton, A., & Sasse, M. A. (2014, July). Desperately seeking assurances: Segmenting users by their information-seeking preferences. In Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on (pp. 102-111). IEEE.

Mousavi, S., Gigerenzer, G., & Kheirandish, R. (2016). Rethinking behavioral economics through fast-and-frugal heuristics. R. Frantz, S.-H. Chen, K. Dopfer, F. Heukelom, & S. Mousavi, Routledge Handbook of Behavioral Economics, 280-296.

Mullainathan,S., and Thaler, R.H.2001. Behavioral Economics International Encyclopedia od Social Sciences, 1st edn, pp.1094-1100. Pergamon.

Müller, Sune Dueholm; Holm, Stefan Rubæk; and Søndergaard, Jens (2015) "Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective," Communications of the Association for Information Systems: Vol. 37, Article 42

Nash, J. (1951). Non-cooperative games. Annals of mathematics, 286-295.

National Research Council. (2007). Engaging privacy and information technology in a digital age. National Academies Press.

Navarra, D. D., & Cornford, T. (2005). ICT, Innovation and Public Management: Governance, Models and Alternatives for eGovernment Infrastructures. ECIS 2005 proceedings, 121.

Neth, H., Sims, C. R., & Gray, W. D. (2016). Rational task analysis: A methodology to benchmark bounded rationality. Minds and Machines, 26(1-2), 125-148.
Neumann, J. V. (1944). Morgenstern, 1944. Theory of games and economic behavior.

Njilla, L. Y., Pissinou, N., & Makki, K. (2016). Game theoretic modeling of security and trust relationship in cyberspace. International Journal of Communication Systems, 29(9), 1500-1512.

Noam, E. M. (1996). Privacy and self-regulation: Markets for electronic privacy. In Privacy and Self-Regulation in the Information Age. National Telecommunications and Information Administration.

Nofer, M., Hinz, O., Muntermann, J., and Rossnagel, H. (2014). "The Economic Impact of Privacy Violations and Security Breaches," Business & Information Systems Engineering: Vol. 6: Iss. 6, 339-348.

Norberg, P.A. Horne, D. R. and Horne. D. A 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs, Vol.41, No.1, pp.100-126.

Noor, T. H., Sheng, Q. Z., Maamar, Z., & Zeadally, S. (2016). Managing Trust in the Cloud: State of the Art and Research Challenges. Computer, 49(2), 34-45.

Noor, T. H., & Sheng, Q. Z. (2011). Trust as a service: a framework for trust management in cloud environments. In International Conference on Web Information Systems Engineering. Springer Berlin Heidelberg: pp. 314-321.

O'Brien, M. K., & Ahmed, A. A. (2016). Rationality in human movement. Exercise and sport sciences reviews, 44(1), 20-28.

O’keefe, D. J. (2002). Persuasion: Theory and research (Vol. 2). Sage.

Olson, J.S., Grudin, J., Horvitz, E., 2005. A Study of Preferences for Sharing and Privacy. In: Conference on Human Factors in Computing Systems. Portland, Oregon, USA, April 2-7, 2005, ACM: USA.

Oscar Diez and Andres Silva, “Cloud computing and Critical Infrastructure Systems”, Proc. of the 2011 6th International Conference on System of Systems Engineering, Albuquerque, New Mexico, USA - June 27-30, 2011, pp. 7-12.

Otterloo, van S. (2005). “The value of privacy: optimal strategies for privacy minded agents”, in Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems (AAMAS ’05), ACM, pp.1015-1022.

Pal, R., & Hui, P. (2013). Economic models for cloud service markets: Pricing and capacity planning. Theoretical Computer Science, 496, 113-124.

Pan, Y., and Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. Journal of Retailing, Vol.82, No.4, pp.331-338.
Parra-Arnau, J., Rebollo-Monedero, D., & Forné, J. (2014). Measuring the privacy of user profiles in personalized information systems. Future Generation Computer Systems, 33, 53-63.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International journal of electronic commerce, 7*(3), 101-134.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go?. *MIS quarterly, 977*-988.

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. In ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, pp.44-52.

Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer London.

Penna, P., Schopppmann, F., Silvestri, R., & Widmayer, P. (2009). Pseudonyms in Cost-Sharing Games. Internet and Network Economics, 256-267.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2-17.

Pieters, W., & van Cleeff, A. (2009). The precautionary principle in a world of digital dependencies. *Computer, 42*(6).

Pitta, D. (2010). Jump on the bandwagon{its the last one: New developments in online promotion. Journal of Consumer Marketing 27 (2).

Pollach, I. (2007)"What’s wrong with online privacy policies?”, Communications of the ACM, vol. 30, no. 5, pp. 103-108.

Posner, R. A. (1981). The economics of privacy. *The American economic review, 71*(2), 405-409.

Post, R. C. (1991). “Rereading Warren and Brandeis: Privacy, Property, and Appropriation”, Case Western Reserve Law Review: Vol41, Article 3.

Raya, M., Shokri, R., & Hubaux, J. P. (2010, March). On the tradeoff between trust and privacy in wireless ad hoc networks. In Proceedings of the third ACM conference on Wireless network security (pp. 75-80). ACM.

Rajbhandari, L. Snekkenes, A. (2011). “Mapping between Classical Risk Management and Game Theoretical Approaches”, Lecture Notes in Computer Science, Springer, Vol. 7025,pp. 147-154 Doi: 10.1007/978-3-642-24712-5_12
Rajbhandari L. and Snekkenes, E.A. (2010). “Using Game Theory to Analyze Risk to Privacy: An Initial Insight”, in Fischer-Hubner et al. (eds), Privacy and Identity 2010, IFIP AICT Vol.352, No.2001, pp. 41-51.

Ralph, P. (2015). The sensemaking-coevolution-implementation theory of software design. Science of Computer Programming, 101, 21-41.

Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. International Journal of Information Management, 36(4), 618-625.

Raisinghani, M., Idemudia, E. C., Chekuri, M., Fisher, K., & Hanna, J. (2015). Cloud Computing in the 21st Century: A Managerial Perspective for. Advanced Research on Cloud Computing Design and Applications, 188.

Rana, N. P., Dwivedi, Y. K., and Williams, M. D. (2015). A meta-analysis of existing research on citizen adoption of e-government. Information Systems Frontiers, 17(3), 547-563.

Read, D. W. (2016). How culture makes us human: primate social evolution and the formation of human societies. Routledge.

Reed, Stephen K. Cognition: Theories and applications. CENGAGE learning, 2012.

Regan, P. M. (2002). Privacy as a common good in the digital world. Information, Communication and Society, 5(3), 382-405.

Rippl, S. (2002) ‘Cultural theory and risk perception: A proposal for a better measurement’, Journal of Risk Research, Vol. 5, No. 2, pp.147–165

Ruiter, J. and M. Warnier, 2011, “Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice”, in Computers, Privacy and Data Protection: an Element of Choice, S. Gutwirth, Y. Poulet, P. De Hert, and R. Leenes (eds.), Dordrecht: Springer Netherlands, pp. 361–376.

Rumelt, R. P., & Lamb, R. (1997). Towards a strategic theory of the firm. Resources, firms, and strategies: A reader in the resource-based perspective, 131-145.

Samarati, P., & di Vimercati, S. D. C. (2016). Cloud security: Issues and concerns. Wiley, New York.

Sander van der Linden (2016) A Conceptual Critique of the Cultural Cognition Thesis Science Communication 2016, Vol. 38(i) p.p 128 –138

Sacharoff, L. (2012). The Relational Nature of Privacy. Lewis & Clark L. Rev., 16, 1249.

Sato, M. (2010). Personal data in the cloud: A global survey of consumer attitudes. Minato-ku, Tokyo 105-7123, JAPAN
Schoeman, F. D. (1992). Privacy and social freedom. Cambridge university press.

Schram, A. J. (2008). Experimental public choice. In Readings in Public Choice and Constitutional Political Economy (pp. 579-591). Springer, Boston, MA.

Seigneur, J. M., & Jensen, C. D. (2004). Trading privacy for trust. In International Conference on Trust Management (pp. 93-107). Vol.2995 Springer Berlin Heidelberg.

Sharma, S. K., & Govindaluri, S. M. (2014). Internet banking adoption in India: structural equation modeling approach. Journal of Indian Business Research, 6(2), 155-169

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. Computers in Human Behavior, 62, pp.61-69.

Schwaig, K. S., Kane, G. C., and Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? Information and management, 43(7), 805-820.

Segars, A.H., Grover, V. (1993) ‘Re-examining perceived ease of use and usefulness: A confirmatory factor analysis’, MIS Quarterly, Vol. 17, No. 4, pp.517–525.

Shiller, R. J. (2015). Irrational exuberance. Princeton university press.

Silcock, R. (2001). What is e-government. Parliamentary affairs, 54(1), 88-101.

Simon, H. A. (1955). A Behavioral Model of Rational Choice. The Quarterly Journal of Economics Vol. 69, No. 1 (Feb., 1955), pp. 99-118

Simon, H. A. (1996). The sciences of the artificial (3rd Ed.). Cambridge, MA: MIT Press.

Simon, H. A. (2010). A behavioral model of rational choice. Competition Policy International, 6(1), 241-258.

Simonson I. Will I like a “medium” pillow? Another look at constructed and inherent preferences. J Consum Psychol2008, 18:155–169.

Snekkenes, E. (2013). Position Paper: Privacy Risk Analysis Is about Understanding Conflicting Incentives. In IFIP Working Conference on Policies and Research in Identity Management (pp. 100-103). Springer Berlin Heidelberg.

Slovic, P. (1987) ‘Perception of Risk’, Science, Vol. 236, pp.280-285.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 35(4), 989-1016.

Smith, H. J., Milberg, J. S., and Burke, J. S. 1996. “Information Privacy: Measuring Individuals’ Concerns About Organizational Practices,”MIS Quarterly (20:2), pp. 167-196.
Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. L. Rev.*, 154, 477.

Solove, D. J. (2006). “A taxonomy of privacy”. *University of Pennsylvania Law Review* 154 (3), 477.

Solove, D. (2008). Understanding privacy.

Som, C., Hilty, L. M., & Köhler, A. R. (2009). The precautionary principle as a framework for a sustainable information society. *Journal of Business Ethics*, 85, 493-505.

Son, J. Y., & Kim, S. S. (2008). Internet users’ information privacy-protective responses: a taxonomy and a nomological model. *MIS quarterly*, 503-529.

Squicciarini CA, Xu H, Zhang X (2011) CoPE: Enabling collaborative privacy management in online social networks. *Journal of Business Ethics*, 85, 493-505.

Stacy, W., & MacMillan, J. (1995). Cognitive bias in software engineering. *Communications of the ACM*, 38(6), 57-63.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49.

Stigler, G. J. (1980). An introduction to privacy in economics and politics. *The Journal of Legal Studies*, 9(4), 623-644.

Subramanian, G.H. (1994) ‘A replication of perceived usefulness and perceived ease of use measurement’, *Decision Sciences*, Vol. 25, No. 5-6, pp. 863–873.

Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52, 278-292.

Svantesson, D. and Clarke, R. (2010) Privacy and consumer risks in cloud computing *Computer law and security review*, 26 (4), pp.391-397.

Tang, J., Zhang, J., Yao, L., Li, J., Zhang, L., & Su, Z. (2008, August). Arnetminer: extraction and mining of academic social networks. In *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 990-998). ACM.

Tang, J., Qu, M., Wang, M., Zhang, M., Yan, J., & Mei, Q. (2015, May). Line: Large-scale information network embedding. In *Proceedings of the 24th International Conference on World Wide Web* (pp. 1067-1077). International World Wide Web Conferences Steering Committee.

Tarhini, A., Arachchilage, N. A. G., & Abbasi, M. S. (2015). A critical review of theories and models of technology adoption and acceptance in information system research. *International Journal of Technology Diffusion (IJTD)*, 6(4), 58-77.
Taylor, C. R. 2004. Consumer Privacy and the Market for Customer Information. Rand Journal of Economics, 35(4): 631-51

Taylor, C.R., Conitzer, V. and Wagman, L. (2010). “Online Privacy and Price Discrimination”, Economic Research Initiatives at Duke Working Paper No. 79, July 2010, Available at http://ssrn.com/abstract=1695143 (last accessed 12 July 2016).

Toplak, M. E., West, R. F., & Stanovich, K. E. (2011). The Cognitive Reflection Test as a predictor of performance on heuristics-and-biases tasks. Memory & cognition, 39(7), 1275.

Toplak, M. E., West, R. F., & Stanovich, K. E. (2014). Assessing miserly information processing: An expansion of the Cognitive Reflection Test. Thinking & Reasoning, 20(2), 147-168.

TRUSTe (2004) TRUSTe plugs into wireless: TRUSTe’s wire less advisory committee announces first wireless privacy standards, http://www.truste.org/articles/wireless_guidelines_0304.php

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2), 254-268.

Tsouh, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Computers & security, 52, 128-141.

Tucker, C. E. (2014, September). Social networks, personalized advertising, and privacy controls. American Marketing Association.

Tucker, C. (2011b). Social Networks, Personalized Advertising, and Privacy Controls. Mimeo, MIT.

Turilli, M., & Floridi, L. (2009). The ethics of information transparency. Ethics and Information Technology, 11(2), 105-112.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. Cognitive psychology, 5(2), 207-232.

Tversky, A., and Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124-1131

Tversky, A., & Kahneman, D. (2016). Advances in Prospect Theory: Cumulative Representation of Uncertainty. In Readings in Formal Epistemology (pp. 493-519). Springer International Publishing.

Varian, H. (1985). Price discrimination and social welfare. The American Economic Review 75 (4), 870(875).
Varian, H., F. Wallenberg, and G. Woroch (2005). The demographics of the do-not-call list. IEEE Security and Privacy 3 (1), 34–39.

Varian, H. R. (1996). Economic aspects of personal privacy. In Privacy and Self-Regulation in the Information Age. National Telecommunications and Information Administration.

Volz, K. G., & Gigerenzer, G. (2012). Cognitive processes in decisions under risk are not the same as in decisions under uncertainty. *Frontiers in Neuroscience, 6*.

Vu, K.-P. L., Chambers, V., Creekmur, B., Cho, D. and Proctor, R. W. (2010). “Influence of the Privacy Bird® user agent on user trust of different web sites”, Computers in Industry, vol. 61, pp. 311–317.

Wang W, Benbasat I (2009) Interactive decision aids for consumer decision making in e-commerce: The influence of perceived strategy restrictiveness. MIS Quart. 33(2):293–320.

Wang, Q., C. Wang, K. Ren, W. Lou, and J. Li (2011) “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” Parallel and Distributed Systems, IEEE Transactions (22)5, pp. 847–859.

Warren, S. D., and Brandeis, L. D. (1890). The right to privacy. In Harvard Law Review vol. 4, pp. 193–220.

Wathieu, L. and Friedman, A, 2005. An Empirical Approach to Understanding Privacy Valuation. Proceedings of the Workshop on the Economics of Information Security (WEIS ’05).

Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Transactions on Vehicular Technology, 63*(9), 4647-4658.

West, R. (2008). The psychology of security. Communications of the ACM, 51(4), 34-40.

Westin, A., (1970). Privacy and freedom. Atheneum.

Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2015). *Engineering psychology & human performance*. Psychology Press.

Wilkinson, N., 2008. An Introduction to Behavioral Economics. Palgrave-Macmillan, Basingstoke, UK.

Wilkinson, N., & Klaes, M. (2012). *An introduction to behavioral economics*. Palgrave Macmillan.

William Petty, J., Scott Jr, D. F., & Bird, M. M. (1975). The capital expenditure decision-making process of large corporations. *The engineering economist, 20*(3), 159-172.
Xu, H., Dinev, T., Smith, J., Hart, P. 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances, Journal of the Association for Information Systems, Vol. 12 Issue 12 pp. 798-824.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. Information Systems Research, 23(4), 1342-1363.

Yildiz, M. (2007) ‘E-Government research: Reviewing the literature, limitations, and waysforward’, Government Information Quarterly, Vol. 24, No. 3, pp. 646-665.

Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. Journal of Internet Services and Applications, 7(1), 1-12.

Young, A. L., and Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Communication and Society, 16(4), 479-500.

Tarhini, A., Teo, T, and Tarhini, T. (2015). A cross-cultural validity of the E-learning Acceptance Measure (ElAM) in Lebanon and England: A Confirmatory Factor Analysis, Education and Information Technologies, DOI: 10.1007/s10639-015-9381-9

Varian, H. R. (1996). Differential pricing and efficiency. First Monday, 1(2).

Venkatesh, V. and Davis, F.D. (2000), “A theoretical extension of the technology acceptance model: four longitudinal field studies”, Management Science, Vol. 46 No. 2, pp. 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: toward a unified view. MIS Quarterly, 425-478.

Vila, T., Greenstadt, R., & Molnar, D. (2003, September). Why we can’t be bothered to read privacy policies models of privacy economics as a lemons market. In Proceedings of the 5th international conference on Electronic commerce (pp. 403-407). ACM

W3C, “The Platform for Privacy Preferences 1.1 (P3P1.1) Specification”, Nov. 2006, available online at: http://www.w3.org/TR/P3P1/ (last access 12 July 2016).

Wallace, P. (2015). The psychology of the Internet. Cambridge University Press.

Wang, Y., Norice, G., and Cranor, L. F. (2011). Who Is Concerned about What? A Study of American, Chinese and Indian Users’ Privacy Concerns on Social Network Sites. In J. M. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, A. Sasse, and Y. Beres (Eds.), Trust and Trustworthy Computing (pp. 146-153). Springer Berlin Heidelberg.

Warren, C., McGraw, A. P., & Van Boven, L. (2011). Values and preferences: Defining preference construction. Wiley Interdisciplinary Reviews: Cognitive Science, 2(2), 193-205.
Wathieu, L., & Friedman, A. A. (2007). An empirical approach to understanding privacy valuation.

Westin A. (1967) Privacy and Freedom. New York: Atheneum, ISBN0370013255, 9780370013251.

Wildavsky, A. (1987) "Choosing Preferences by Constructing Institutions: A Cultural Theory of Preference", The American Political Science Review, Vol. 81, No. 1, pp. 3-22

Wixom B.H. and Todd P. A. (2005) ‘A Theoretical Integration of User Satisfaction and Technology Acceptance’, Information Systems Research, Vol. 16, No. 1, pp.85-102.

Wong, A., Welch, C. J., Kuethe, J. T., Vazquez, E., Shaimi, M., Henderson, D., ... & Hughes, D. L. (2004). Reactive resin facilitated preparation of an enantiopure fluorobicyclocoketone. Organic & biomolecular chemistry, 2(2), 168-174.

Wu, Y., Cegielski, C.G., Hazen, B.T. and Hall, D.J. 2013. Cloud computing in support of supply chain information system infrastructure: understanding when to go to the cloud, Journal of Supply Chain Management 49, pp. 25–41.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12(12), 798.

Yadav, A. K., Tomar, R., Kumar, D., & Gupta, H. (2012). Security and privacy concerns in cloud computing, International Journal of Advanced Research in Computer Science and Software Engineering, 2(5), pp. 379 – 383.

Yang, H. and Tate, M. (2012) "A Descriptive Literature Review and Classification of Cloud Computing Research,"Communications of the Association for Information Systems: Vol. 31, Article 2

Yildiz, M. (2007) 'E-Government research: Reviewing the literature, limitations, and ways forward', Government Information Quarterly, Vol. 24, No. 3, pp.646-665.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.

Zorrilla, M. and García-Saiz, D. 2013. A service oriented architecture to provide data mining services for non-expert data miners, Decision Support Systems 55 pp.399–411.
Publications

**Journal Articles**

Jo. Kokolakis, S., Anastasopoulou K, Tryfonas, (2016) “Consumer Trust in Cloud Services and the Role of Security Certification: A Game-Theoretic Analysis” (working paper)

J1. Anastasopoulou K, Tryfonas, T. and Kokolakis, S. (2015) ‘Strategic stakeholder interaction analysis of cloud-based mobile applications uses of privacy-sensitive end users’, *Universal Access in the Information Society*  
[http://www.springer.com/computer/hci/journal/10209](http://www.springer.com/computer/hci/journal/10209) (to appear).

J2. Anastasopoulou K, and Kokolakis S. (2013) ‘Exploring Citizens’ Intention to Use e-Government Services: The Role of Cultural Bias’, *International Journal of Electronic Governance*, Vol. 6, No. 1, pp. 3-19.

**Refereed Conferences with Proceedings**

C1. Anastasopoulou K., Kokolakis, S. and Tryfonas T. (2013) ‘Strategic Interaction Analysis of Privacy-sensitive end-users use of cloud based mobile apps’ (abstract refereed), 15th *International Conference on Human-Computer Interaction (HCII2013)*, 21-26 July 2013, Las Vegas, Nevada, USA.

C2. Kokolakis, S. Anastasopoulou K, and Karyda, M. (2012) ‘An Analysis of Privacy-related Strategic Choices of Buyers and Sellers in e-Commerce Transactions’, 16th *Panhellenic Conference on Informatics (PCI2012)*, 5-7 October 2012, Piraeus, CPS.

C3. Loukis, E., Kokolakis, S. and Anastasopoulou K. (2011) ‘Factors of PKI adoption in European firms’, *The 6th Mediterranean Conference on Information Systems (MCIS 2011)*, 3-5 September 2011, Cyprus.

**Refereed Posters**

P1. Anastasopoulou K., Kokolakis, S. and Tryfonas T. (2012) ‘Analysis of strategic stakeholder interactions in cloud-based mobile app use by privacy-sensitive end users’, *Conference on Decision and Game Theory for Security (GameSec2012)*, 5-6 November 2012, Budapest, Hungary.

---

1 A preliminary version of this paper appeared in the Proceedings of the 15th International Conference on Human-Computer Interaction (HCII2013).
