A Behavioural Analysis of Online Privacy and Security

Michelle Baddeley

July 2011

CWPE 1147

A Behavioural Analysis of Online Privacy and Security

Michelle Baddeley

Gonville and Caius College, University of Cambridge, UK [*]

July 2011

Abstract

Psychological and sociological factors constrain economic decision-making in many contexts including the online world. Behavioural economics and economic psychology emphasise that people will make mistakes in processing information and in planning for the future; these mistakes will also distort learning processes. Emotions and visceral factors will play a key role - not only affecting people's actions but also distorting the interactions between information, learning and choices. This will have wide-ranging implications for online behavior and information security management, making people more vulnerable to security/privacy abuses including hacking, spam attacks, phishing, identity theft and online financial exploitation. These vulnerabilities raise crucial policy questions - recently made more pressing in the light of recent phone-hacking scandals in the UK. This paper outlines some of the behavioural factors affecting people's online behaviour and analyses real-world reactions to online fraud using evidence from the British Crime Survey 2009-10.

Keywords: behavioural economics, information security, online fraud, cognitive bias

JEL codes: D03,D18,D83,K42

1 Introduction

As more and more human activity is concentrated in the internet, pressure grows on financial information systems to adapt to the increased volume of online activity, including banking / shopping and social networking. Electronic monetary instruments including electronic cash and mobile payments are proving to be potentially superior substitutes for conventional monetary instruments but significant problems have emerged. Alongside the positive innovations, technological innovations have facilitated significant abuses such as anti-social behavior; security/privacy abuses including hacking, spam attacks, phishing, identity theft; and vulnerability to online exploitation e.g.

[*]Contact details: mb150@cam.ac.uk, Gonville and Caius College, Cambridge CB2 1TA

online payday loans. Data from IC3 shows that growth in violations has increased rapidly; complaints to the US Internet Complaint Crime Center about online vulnerabilities, including mass market fraud, online lotteries, charity hoaxes etc. etc., grew at an annualised rate of 33% per annum between 2000 and 2010 (Source IC3 Internet Crime Report 2010, p 8).

Whilst there are technical dimensions and solutions to these problems, the most effective solutions will have to address the realities of real-world human behavior. This raises some crucial policy questions, made more pressing in the light of recent phone-hacking scandals in the UK. To what extent do individuals control for themselves the personal and financial information that they release to the world via email and the internet? To what extent should governments intervene to prevent abuses? To inform our understanding specifically about what individuals can do to protect themselves in a computerised world, this paper outlines and analyses empirically some of the economic and behavioural constraints which will affect online behaviour.

In addressing these questions, the first section of this paper outlines some of the economic factors affecting online vulnerability; the second section extends the analysis by outlining some of the behavioural constraints on online behaviour. Empirical patterns are explored in section 3 using data from the British Crime Survey 2009/10 analysed using least squares and binary dependent variable estimation techniques. Conclusions and policy implications are outlined in section 4.

2 Online vulnerability in rational choice models

Do people have the inclination and/or ability to protect themselves from fraud and other security violations? In answering this question, mainstream economics focuses on models of behaviour which assume that people are selfish, independent maximisers. Informed by objective factors, they are driven by mathematical judgements about the relative benefits and costs of their choices and not by more diffuse, subjective psychological and sociological forces. The policy implication is that individuals should be left to decide for themselves whether or not they need protection.

Whilst the simplifying assumptions underlying standard economic solutions generate a clear and simple model of human decision-making, this model often lacks realism and empirical validity. It assumes markets and behaviour which are perfect, on average at least, and it is difficult fully to understand within this stark approach the range of issues relevant to security and human behaviour. Nonetheless a few themes can be illuminated via modest adaptations to the standard economic model, once sources of market failure are incorporated into the model, e.g. imperfect competition, network effects and network externalities, public goods and price discrimination.

2.1 Information security and market failure

In the interactions between computer security and human behavior market failures will be endemic, exacerbated by the fact that online activity is dominated by networked goods. Network externalities, high fixed costs, low marginal costs and lock-in all suppress competitive pressures and sustain oligopolistic industrial structures. Forces of imperfect competition are encouraged further by the complementarities that emerge because networked products are often consumed in bundles especially if they have little value in isolation. Consumers of electronic money products for example will be looking for a system that supports their electronic payments and so compatibility and operating standards incorporating security are important. Complementarities between different elements of computerized systems, e.g. between CPUs and OSs, will generate pressures for producers to merge, increasing oligopolistic tendencies [86]. Other distinctive but related characteristics of networked goods including externalities and switching costs will further limit competitive pressures [51], [76], [36]. Network externalities emerge because the utility derived - for example, from the use of an electronic payment system - is dependent upon the fact that other consumers are using the same system; but at the same time, the value of access to additional users of the internet is generally very small and so the costs involved are not easily justifiable for the individual. In an online context for example, the additional value to an individual of signing up to an electronic payment system will be small especially if other consumers are not using the same payment system [51], [36]. Paralleling microeconomic models of road use, private incentives generate multiple equilibria including extremes of congestion versus under-use: a producer may attract all the potential consumers within the network - or none of them. PayPal is an example of a system which attracts many consumers just because other consumers are using it; DigiCash was a system which attracted few consumers and so could not reach the critical mass required for it to survive. Use of the digital currency Bitcoin is growing but remains constrained by its limited acceptability.

For electronic payment networks to grow and acceptability to widen, in theory at least, the security and reliability of a system should enhance its acceptability. However, Bonneau and Preibusch (2009) analyse evidence about social networks which shows that, whilst the industry is vigorously competitive, privacy is not always a selling point for the ordinary user even though it may be a concern for hawkish privacy experts [27]. This generates privacy communication games in which the privacy hawks are kept happy whilst privacy issues are hidden in order to maximise sign-up, generating a dysfunctional market for privacy in which privacy is undersold. Further evidence of dysfunctional privacy markets comes from experimental studies; Beresford et al. (2010), using experimental data, found that people are just as likely to buy DVDs from an online store asking for more sensitive data as they were to buy from a store not asking for this information, even when the prices charged by the two stores were the same [24]. The negative impacts of individuals' neglect of their own privacy are magnified because of commercial incentives to erode privacy: given heterogeneous and shifting preferences, there are commercial incentives to price discriminate and these will be enabled by the decreases in online privacy which have accompanied the growth of online social networks. Decreased privacy has fostered price discrimination by enabling producers to target individual customers in different ways [10], [11].

Switching costs and lock-in may apply e.g. if exiting a payment system is relatively more costly than entering it [68]. This is a characteristic that applies to an extent to PayPal because it is easier to set up an account with PayPal than to close the account and sign-up for an alternative payments system. Economies of scale will mean that whilst there are high sunk or fixed costs involved e.g. in developing an electronic payments infrastructure, the marginal costs of copying and distributing electronic payment devices or tokens will be low. This generates a natural monopoly in which the average cost function declines sharply and limits the operation of competitive forces. These limits are likely to be more important for electronic systems if the costs of developing new privacy and security infrastructure have to be borne by private institutions.

Network externalities are also linked to the fact that security is a quasi public good. From consumers' points-of-view, if others in the network are adopting security controls which disable and deter a large volume of fraudulent activity, then there is no incentive for an individual to adopt those security controls themselves. When a network is already highly secure, then that security provision exhibits many of the key characteristics of a public good *viz.* non-depletability - the provision of a good or service does not diminish because of consumption by an additional person; non-rivalry - consumption by one person does not preclude consumption by others; and non-excludability - no one can be prevented from consuming the good. This means that, in common with other public goods, a secure internet is susceptible to the free-rider problems: consumers are able to free ride on the benefits of others' cautiousness without incurring any of the costs, generating a Prisoner's Dilemma type outcome [10] [11].

2.2 Asymmeric information and principal-agent problems

Standard economic models can be adapted to incorporate the market failures associated with imperfect/ asymmetric information and misaligned incentives. For example, as Akerlof's lemons principle illustrates, markets which are prone to adverse selection problems are "thin"; fewer transactions take place because prices reflect average product quality creating a disincentive to supply good quality products [6]. Unless signalling or screening mechanisms can be developed effectively to communicate information about product quality, the bad quality products will drive down prices and driving out good quality producers. In the context of security and human behaviour when people select technical products to protect their privacy and security, as the technical sophistication of products increases the ordinary consumer has far less information than the vendors about how effectively these products will work. Fundamental uncertainty may mean that even the vendor does not know how secure their software is in practice. Whilst to an extent these problems might be overcome by learning (explored below), the search costs of investigating privacy products available are likely to be very high. A standard way to overcome adverse selection problems is to devise a certification system but if the dubious firms are the ones buying certification and/or if all firms are buying the easy certification then certification is unlikely to lead to efficiency gains [11].

Asymmetric information will also generate post-contractual problems of moral hazard and hidden action. If agents' incentives are misaligned and the principal cannot effectively monitor the efforts of their agent, the agent has incentives to cheat e.g. a firm providing security products aims to maximise profits and minimise costs; the consumer wants the best protection they can afford but most consumers cannot monitor effectively whether or not their ISP or social network is (cost effectively) doing what they promise to do. Principal-agent problems are also relevant for aspects of online behavior that involve team efforts, e.g. security protection often depends on the efforts of many agents and the outcome may depend on either the minimum effort, best effort or aggregate effort [11] [86] [47]. For teamwork affecting security threats it may be difficult to identify who is responsible for responsible versus irresponsible online behaviour, e.g. when opening emails each member of the online community will have an incentive to free-ride on the responsible behaviour of others, thus generating a Prisoner's dilemma game in which collective efforts to promote internet security are constrained. For the individual, the consequences of minimum effort are not dissimilar from those from best effort and aggregate effort so, overall, limited efforts will be made, increasing the vulnerability of online networks to attacks.

3 Behavioural constraints

The security issues discussed above are analysed within a rational choice approach, allowing market failure but nonetheless retaining a standard economic model which just allows that behaviour is constrained by imperfect information and market failures. In reality, limits on rationality are likely to be profound because the world is mutable, complex, uncertain and so socio-psychological forces will have particular traction in constraining rational choice.

Herbert Simon softened economists' conceptions of rationality to allow for uncertainty by introducing the concept of bounded rationality and distinguishing substantive rationality from procedural rationality [77] [15]. If people are assumed to be substantively rational then they are able to form quantifiable expectations of the future and will maximise utility using constrained optimisation techniques to balance marginal benefits with costs. If different people have access to the same information set, then on average, they will form identical expectations centred about some objective probability distribution of outcomes. They will be forward looking incorporating a stable rate of time preference into their decision-making process. If individuals' rationality is bounded in the sense of being constrained by imperfect information, cognitive limitations, and/or time pressures then the sensible application of clear and objective mathematical rules will be difficult because the existence of immeasurable uncertainty precludes the quantification of probabilities of future events.

Bounds to rationality will limit opportunities for substantively rationality behavior in which goals and constraints are quantifiable, enabling the use of mathematical algorithms to guide decision-making. By contrast, procedurally rational behaviour is more likely given uncertainty because it is based on a broad reasoning process rather than the achievement of given representative agent's goals [77]. Procedural rationality is more likely to be associated with satisficing (ie sticking with the current situation because it is comfortable even if it is not an optimum) and involves blunter, broader approaches to information-processing and decision-making. Given the many uncertainties that characterize the ordinary person's online world, online behaviour is more likely to be procedurally rational than substantively rational and many of the behavioural constraints addressed below are consistent with procedurally rational behavior.

3.1 Risk and uncertainty

In using the internet and in particular when using an online payments system or an online social network, consumers must form an expectation of the likelihood of the information that they reveal will be used against them in some way in the future, eg via online fraud, being fired or ostracised for indulging in indiscrete online gossip, becoming susceptible to identity theft. This raises the problem of capturing how people deal with risk and uncertainty when making choices that have future consequences. Some assumption or hypothesis must be made to capture how people form these expectations about the future. The extent to which it is possible to assign such a number will be determined by whether the situation is one of Knightian risk or Knightian uncertainty [53]. Events governed by Knightian risk tend to be repeatable and the outcome of a deterministic and immutable data generating mechanism, such as an unloaded die or a lottery machine. Under Knightian uncertainty people can say no more than that an event is probable or improbable; they cannot assign a number or ranking in their comparison of probabilities of different events. Events characterised by Knightian uncertainty are more common than those characterised by Knightian risk, at least in the economic and social sphere. Economic events are often non-repeating, occurring under conditions that cannot be controlled. Errors in expectations will be non-random and will not cancel out. Instead they may spread generating systematic trends.

Approaches which assume repeatable events, complete information and/or an understanding of the data-generating mechanism will be of little use in understanding online behavior. First, information is incomplete and the data generating processes dictating outcomes will often be unknown to the individual. Secondly, online decisions may often be about nonrepeatable, unprecedented events (e.g. buying from a new eBay trader) and this means that information about past outcomes will be of little use. Prediction is particularly complex when it comes to economic processes because the economic world is mutable: peoples' beliefs about economic structure have the capacity to change that economic structure, as emphasised in the mainstream macroeconomic literature on dynamic inconsistency [57] and the heterodox literature on non-ergodicity [33]. Reality changes as expectations change: expectations affect economic events which in turn determine expectations, e.g. a network will grow because people believe it will grow because it is growing. Endogeneity will mean that events and beliefs about the system determine the path of that system [71], [72], [73] e.g. in an eBay auction a price may go up just because people believe it will go up. Future outcomes will be affected by current decisions based on expectations of the future formed today: inter-temporal feedbacks between past, present and future will determine reality. As new information accumulates rapidly within large online communities a complex multiplicity of outcomes is possible and it will be impossible to form a single objective judgement of possibilities, undermining even more subjectively based Bayesian probability concepts.

Whilst these problems can be addressed to an extent using Bayesian models there are a number of problems with the Bayesian approach. First, there are practical problems in its application, e.g. in economics, there is often a paucity of data that can be used to quantify subjectively formed probability judgements [52]. Also, standard economic models assume that economic decision-making is highly formalised and, particularly in an online environment, people do not cope well with formal methods [63]. Human intuitive cognitive processes do not deal well with more flexible Bayesian thinking methods either. For online behavior, an ordinary individual's knowledge of his/her online world is likely to be incomplete and so it will be difficult if not impossible to calculate statistical probabilities based upon past frequencies. Online decision-making is more likely to be governed by subjective / inductive judgements: a decision to buy an innovative but relatively expensive virus protection software package is not like dealing a card from a pack of 52 cards or buying a lottery ticket when you know that one million tickets are being sold. Other implications for security and human behaviour relate to legal issues, e.g. in insuring against the consequences of a spam attack for example, the basic principle would be that risks should be borne by those who control the risk [10] [11] but for decisions relating to internet use, the risks are interdependent, uncertain and to an extent unknowable; this profound uncertainty means that it is difficult to design efficient insurance to protect against online vulnerabilities.

3.2 Learning and social influence

Learning is an essential aspect of rational behavior and given the esoteric and technical nature of many aspects of online activity, learning processes will be important. For computer privacy and security, learning is crucial because it determines how people adapt to innovative new technologies which may have many unfamiliar aspects. Learning can be captured in a limited sense by allowing that people search efficiently for information, i.e. will search for more information whilst the marginal benefits exceed the marginal costs of that information. Behavioural economics has enriched economists' conceptions of learning by building on insights from behaviourist psychology about conditioning, as developed in reinforcement learning models. Economists have also developed belief learning models focussed on the processes by which people form beliefs about the actions of their opponents. Another important form of learning that is receiving increasing attention in behavioural economics is social learning. Without an objective path to follow, it may be procedurally rational to follow the crowd and/or to learn from past output signals about what others are doing [83], [1]. Keynes argues that when your information is sparse you will do what others do because perhaps they have better information [53], [54] [55] [56]. In Keynes's analysis, such herding behaviours can be linked to probabilistic judgements in a Bayesian setting. Differences in posterior judgements of probable outcomes may not reflect irrationality but instead may emerge as a result of differences in prior information. Rational economic agents may have an incentive to follow the crowd and herding will result as a response to individuals' perceptions of their own ignorance. Herding will be rational if an individual has reason to believe that other agents' judgements are based upon better information than their own: other people's judgements become a data-set in themselves. In this way, people will incorporate others' opinions into their prior information set and herding tendencies reflect posterior judgements of probabilities, see also Sharfstein and Stein (1990), Banerjee (1992) and Bikhchandani, Hirschleifer and Welch (1992) and Chamley (2003) amongst others [69] [18] [21][22][30].

Social learning may also reflect broader social influences whether normative (e.g. peer pressure) or informational (e.g. learning from others' actions in a non-Bayesian sense). Shiller (2000, 2003) analyses these ideas in the context of feedback theories of endogenous opinion formation in which beliefs about the system determine the path of that system [72] [73] [83] [28] [80]. Similarly, social influence can be described using evolutionary biological analogies, e.g. those based around the concept of memes - the cultural analogy of genes [34]. Imitation is a distinguishing characteristic of human behaviour and so a meme can be understood as a unit of imitation [25]. The discovery of 'mirror neurons' (neurons in the pre-motor areas of primate brains that are activated without conscious control and generate imitative behaviour in primates) has lent some scientific support to biological explanations for imitative behaviour [66]. This biological approach is compatible with neural network theories of information processing, i.e. mathematical approaches that emulate adaptive learning processes observed in human brains. Successful memes survive if they are remembered and will reproduce when they are transmitted effectively between people. So memes are more likely to survive when they map effectively onto human cognitive structures, incorporate a standardised decision structure and/or have been reinforced by dominant members of the scientific community [9].

The implications for privacy and security are that individuals' behavior is likely to be determined by the actions of others for example people will be more likely to adopt protections and controls if others in their online and offline networks are doing the same. The online environment does allow information to accumulate rapidly about the relative reliability of traders and products, e.g. via online review sites and this is likely to foster social learning processes. Also, if group leaders can be identified and encouraged to adopt appropriate online protections then others will follow their example. If information about the adoption of safeguards by others is prominent then this social influence will encourage people to do what others are doing and cooperation between self-seeking individuals will lead to the evolution of new social norms [13]. The impact of social norms and social influence has been identified in the context of household energy choices [74] [82] and similar influences may operate in the online environment too. Social influences reflecting investments in social capital, cooperation, trust and reputation will also affect online behaviour. For security and human behaviour, decisions are made in a multidimensional space and reflect contradictory goals and so trust and control are central; effective security and privacy systems will allow transparent communication between trusted parties but will be closed to the "bad guys" [31]. Different social norms about privacy and security will evolve reflecting the speed and anonymity of online worlds - for example, it is widely believed that the younger generation is more vulnerable to identity theft because they are far more willing to reveal important personal information. In terms of policy implications, it is possible that, over time, social norms about protecting privacy and security can be encouraged to evolve in various ways including advertising, sanctions and rewards.

3.3 Cognitive bias and heuristics

As noted above, the behaviour of the procedurally rational person does not involve constrained optimisation. Instead, Simon observes that people may be guided by "appropriate deliberation" and decision-making processes will depend on the circumstances. A procedurally rational person will use common sense rather than complex mathematical techniques in assessing their current and future choices. In an uncertain world, actual experience may be surprising by comparison with expectations because an imperfect image of the future has been formed in advance (Shackle 1953, Basili and Zappia 2009) [67], [23]. If people are procedurally rational and the logical link between objective and subjective probabilities is broken, then a range of choices may be defensible. In contrast to the substantive approach, different people, even if they are using the same information, will form different expectations reflecting arbitrarily assigned margins of error. But if expectations turn out to be wrong, is it because people are misguided or is it because the economic reality changed unexpectedly? A large literature has developed analysing the first possibility - that cognitive limits on human information processing mean that individuals' subjective probability estimates are fallible [85] [17]. If the second possibility holds true, will any predictive tool be unequivocally superior to all others? If complexity and endogeneity operate within limits, then the solution may lie with predictive tools that incorporate fuzzy logic methods, in which the binary concepts of 'true' and 'false' are replaced by degrees of truth.

Following from above, research on prospect theory shows that the standard approach to subjective utility has many limitations [50]. Most ordinary people make common mistakes in their judgements of probabilities (e.g. Anderson 1998) [17]. This links into bounded rationality because it reflect limits on the processing ability of the human mind [48] [84] [9]. Inconsistencies may stem either from individual biases or group biases. At least two categories of individual bias can be distinguished: motivational bias and cognitive bias [78]. Motivational biases reflect interests and circumstances and may link into the principal-agent problems outlined above. They can often be significantly reduced with clearly defined tasks and incentive structures. Overall, motivational biases are less of a problem; they can be controlled because they are often under rational control.

Cognitive biases are more problematic because they emerge from incorrect, often unconscious, information processing. Framing effects are a key source of cognitive bias and capture how people's responses will be determined by the way / context in which questions or problems are framed. For example people may exhibit disproportionate aversion to losses relative to their appreciation of gains and so if warnings about the consequences of careless internet behaviour are framed in terms of the losses of irresponsible behaviour rather than the gains from being responsible, then they may be more effective. Also, there will be individual differences in personality traits and other characteristics which may lead some people to be overconfident about their knowledge and overoptimistic about future events, e.g. victims of online scams may be overconfident about their ability to distinguish a scam from an genuine opportunity. Overconfidence is especially problematic for extreme probabilities which people tend to find hard to assess. This will be relevant for computing decisions: in the absence of meaningful and available information about security threats, people will be overly sanguine, for example about their vulnerability to identity theft, and this will be moderated by personality traits and predispositions which correlate with risk intelligence [41]. A lot of electronic and/or online activity is done anonymously and so depersonalisation may also play a role e.g. fraud may be more likely if victims are depersonalized and reduced by perpetrators to nothing more than a credit card number [8].

Many other cognitive biases have been identified too including familiarity and status quo biases, attribution error, endowment effects and loss aversion [59]. Some which may specifically affect online behavior include endowment effects and status quo bias.

Endowment effects in which people overvalue an object because they own it may affect minimum prices on online sites such as eBay. Acquisti (2004) and Acquisti and Grossklags (2006) explore a number of other biases specifically affecting online behaviour including people's tendency to prefer the current situation generating status quo bias, a phenomenon also explored by Thaler and Sunstein in a range of contexts [2] [3] [82]. Some of these biases can be manipulated to encourage people to engage in more efficient behaviour - for example status quo bias, which is about the fact that people tend to favour the existing situation and will tend to avoid the effort involved in changing their choices. Setting online default options cleverly can exploit this bias e.g. if the default option is the maximum privacy protection then a large number of consumers may procrastinate in changing these options thus giving them default protection from security violations.

Cognitive biases also emerge from the use of heuristics, i.e. common-sense devices or rules of thumb derived from experience. In general terms, it may be procedurally rational to use simple heuristics because they allow people to make relatively quick decisions in uncertain situations. They are used because a full assessment of available information is difficult and/or time consuming or when information is sparse. For example, when thinking about buying new software, an ordinary person may have little real knowledge about what is going to happen in the future; given this limited information, they may rely on heuristics to decide. Following the crowd, as discussed above, can be seen as a learning heuristic which sometimes will lead individuals to the wrong decision generating herding externalities. There are a number of other types of commonly employed heuristics that produce cognitive bias including availability, anchoring and adjustment, representativeness, and control [49] [84]. Availability is a recency effect; it is the heuristic of judging an event to be more likely if occurrences of the event can be recalled with relative ease. This may enable quick decision-making but is biased by the prominence of certain events rather than the actual frequency with which these events occur, especially if the event has had a lot of attention in the news. For example, headline news of airplane crashes will be brought to mind more readily than bike crashes, even though the latter are far more frequent. This suggests that economic decisions are affected by memory. Learning and forgetting have particular implications for online security because the modern online world requires memory, most significantly the memory challenge of remembering a large number of passwords. Privacy and security are affected by memory lapses especially because online vulnerability increases each time someone has to change their password because they have forgotten it. This generates a trade-off because password entropy, i.e. the best passwords are unpredictable, is negatively related to memorability: unpredictable passwords are harder to remember [32]. Behavioural economics potentially offers some lessons because forms of forgetting are captured within economic models of learning including belief learning models of weighted fictitious play in which recent experiences are given greater weight than more distant experiences and also in Erev and Roth's reinforcement learning model which incorporates forgetting as an adjustment parameter on past events [40].

For security and human behaviour, the availability heuristic combined with an overoptimism bias may lead people to decide that security is not a problem because they haven't had a problem with it in the recent past, but if recent news stories have focussed on security risks then people may be disproportionately focussed on protecting their security, e.g. recent stories about firesheep, cloud computing and unsecured information sharing might encourage more people to be careful about how they use privacy settings on facebook and twitter.

Anchoring and adjustment is a single heuristic that involves making an initial estimate of a probability, and then revising or adjusting it up or down in the light of new information [84]. This typically results in assessments that are biased towards the anchor value. Anchoring effects may operate in a social dimension if one individual's judgements is 'anchored' to others' opinions [84] [37]. If someone's friends and colleagues are all talking about the benefits of some new software, then a person's judgement of that software may be anchored around these opinions.

Lynch (1996, 2003) connects bias with social influence and the evolutionary replication of ideas arguing that 'thought contagion' affects a wide range of human behaviours and beliefs [60], [61]. Social learning, as discussed above, may interact with individual biases when group interactions generate more complex forms of bias because people are interacting and copy each other thus spreading misjudgements quickly through groups of people. Cognitive biases may lead people to over-estimate each probability in a set of exhaustive and mutually exclusive scenarios and they do not correct probability estimates when the set of exhaustive but mutually exclusive outcomes is augmented, leading to an estimate of total probability in excess of one. Judith Anderson argues that these types of probabilistic mistakes reflect the nature of memes [9]. The problem originates in the input format of data, and in algorithms used; but if prompted by clear signals, the human brain is able to deal with probabilities more effectively. For example, if students are asked to judge the probability of two coincident events within the context of a statistics class, then they will know what to do. However, if outside their classes they are confronted with a problem requiring probability judgements for a situation in which it is not obvious that this is what is required, then they may make an instinctive, intuitive judgement generating statistical mistakes [58]. Anderson suggests that Bayesian approaches could be refined by blending frequentist methods with mental, visual imagery and graphic display - an insight that could have many applications for online environments which enable the use of complex imagery - at the extreme in virtual reality environments. Using these innovations may enable people to avoid online vulnerabilities by enabling human cognition to process probabilistic information more effectively.

The impacts of cognitive bias will be conditioned on broader psychological factors and psychological factors will have an independent impact too. Aside from cognitive bias, analyses of real-world behaviour often reveal that people's decisions are driven by non-rational, unsystematic forces such as gut feel [46], [45]. Gigerezner and Goldstein argue that gut feel and other heuristics are fast and frugal decision-making tools [45], [46]. Biases and heuristics may just be procedurally rational but blunt decision-making tools i.e. a way to use information roughly to cut costs and save time. This does not necessarily imply that behaviour is stupid or misguided, e.g. gut feel and animal spirits may drive positive entrepreneurship when Keynes's animal spirits - spontaneous urges to action overwhelm objective pessimism [55] [14], see also Akerlof and Shiller's broader analysis of animal spirits [7]. Many of these non-rational forces are caught up with socio-psychological motivations and whilst these are woolly concepts and therefore difficult to analyse, there is increasing evidence that they are relevant (e.g. see Loewenstein's analysis of animal spirits). Akerlof and Shiller also focus on the impact of corruption which often grows during boom phases but builds fragility into a system making it vulnerable to instability; this may have online parallels because with the growth of the internet and mobile networks have grown, the motives and opportunities for online crime have grown concomitantly whilst at the same time increasing the fragility of the system.

3.4 The role of emotions

The impact of behavioural constraints on online behaviour will be affected by emotional states. There is a growing literature exploring the role of emotions in economic decision-making [38],[39],[16]. The impact of emotions on human decision-making can be used to pull together the wide ranges of concepts and ideas explored in behavioural economics, economic psychology and neuroeconomics. Neuroeconomics also has a lot to offer in increasing our understanding of the neurological foundations of reward processing and risk [70]. It also escapes specious distinctions between rational, irrational and non-rational behaviour and enhances our understanding of evolutionary processes / proximate mechanisms, e.g. those that generate temptation and procrastination, as discussed above. Emotions can be addressed in different ways and the emotional factors most likely to be relevant to online behavior are the occurrent emotions, i.e. emotions that are generated jointly caused by dispositions and events and so are generated in a particular context [39]. Emotional states more broadly will affect decision-making processes, i.e. when people are in a hot emotional state, then they are more likely to act impulsively [20]. In the online world generally, actions can be implemented at very rapid speeds which means that fast moving, quick decision-making based on the overriding of reason by emotion may lead to a range of self-defeating behaviours. A disposition towards implusivity is triggered in online environments because decisions can be implemented so quickly, e.g. when participating in online gambling and online trading.

Emotions will have an impact on information acquisition, learning in response to new information and the choices which emerge from learned responses and these paths from information through learning to action and the constraints upon them are captured in in Figure 1.

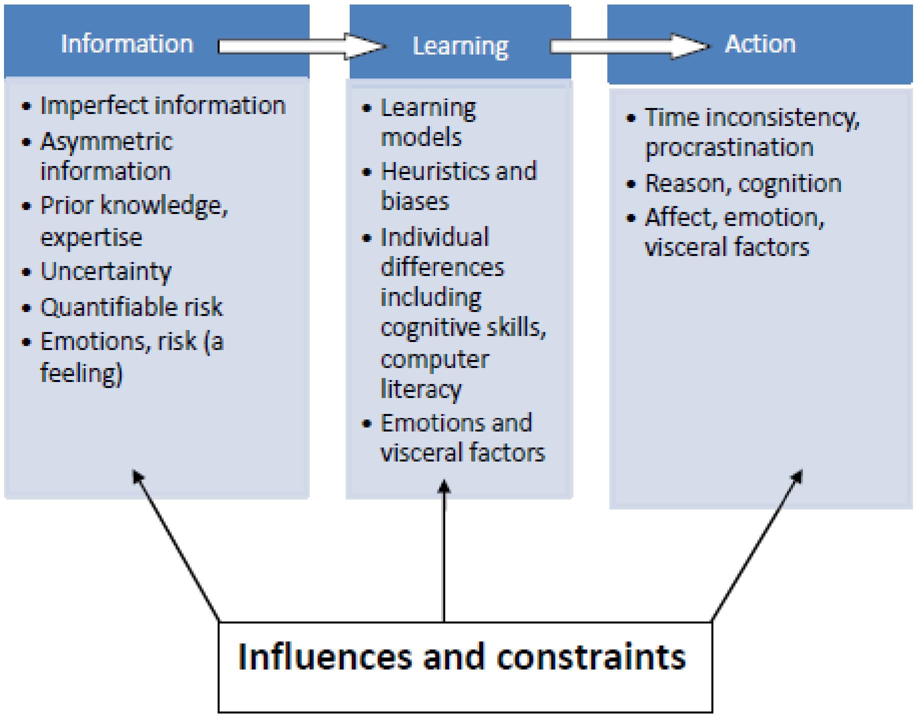
Information
- Imperfect information
- Asymmetric information
- Prior knowledge, expertise
- Uncertainty
- Quantifiable risk
- Emotions, risk (a feeling)
Learning
- Learning models
- Heuristics and biases
- Individual differences including cognitive skills, computer literacy
- Emotions and visceral factors
Action
- Time inconsistency, procrastination
- Reason, cognition
- Affect, emotion, visceral factors
Influences and constraints

Figure 1: Stages of information gathering, learning and action

In acquiring information, emotions will affect subjective perceptions of information e.g. perceptions of risk will be affected by emotional states. Slovic et al (2004) argue that risk itself is a feeling when it is a intuitive, instinctive response to immediate danger [79]. Minsky (1997) analyses emotional constraints arguing that the 'negative knowledge' associated with some emotional states may inhibit whole strategies of thought [62]. When processing of information learning processes are affected by cognitive limitations. Susceptibility to cognitive bias may be affected by emotional responses: people in a happy mood are more likely to use heuristics associated with top-down processing, i.e. relying on pre-existing knowledge with little attention to precise details. By contrast, people in a sad mood are more likely to use bottom-up processing heuristics, paying more attention to precise details than existing knowledge [75]. Emotions have also been shown to affect learning processes in computer based learning environments [4] [5]. As learning is translated into action, emotions and visceral factors will again have an impact because observed behaviour will be the outcome of an interaction between reason and cognition versus emotion and affect. Personality will play a role because personality may generate predispositions to particular emotional states and effective privacy and so security systems could be tailored to suit different personality types [11].

3.5 Time inconsistency, temptation and procrastination

A specific type of decision-making bias with particular relevance for online behavior is present bias emerging from time inconsistency. People's behavior may be inconsistent over time when plans to do something constructive in the future (e.g. backing-up files) change as the future becomes the present because people procrastinate and they lack self control [64] [65] [35]. This can be captured theoretically by a small tweek to the standard economic assumptions about exponential discounting; by introducing a present bias parameter into standard discount functions, preference reversals and time inconsistency can be captured analytically. There is a wide literature demonstrating the relevance of present bias to a wide range of microeconomic and macroeconomic behaviours [44] [12] [42] [82]. Present bias may not be irrational and may reflect a procedurally rational approach, for example if people are treating different financial decisions in different ways by allocating them to different 'mental accounts'. Experimental evidence shows that people, experiencing a windfall gain of $2,400, will save different proportions depending on the circumstance of the windfall and the context in which the windfall is received: they spend $1,200 if the windfall is spread over a series of monthly payments, $785 if they receive a single lump sum and nothing if is an inheritance. Thaler argues that this is because rather than treating economic decisions together as a single gigantic maximization problem people assign different events to separate mental accounts [81].

Acquisti and Grossklags have analysed the implications of present bias for people's choices about privacy and security building on the behavioural economics literature on procrastination and self control [2] [3]. When using the internet people will procrastinate about setting up effective security systems in much the same way as many people procrastinate about backing-up files. Procrastination is potentially a key policy issue particularly if the most effective privacy and security solutions are to be driven by individual choices. Models of temptation are also explored in behavioural economics [43] and the temptation and procrastination models can be spliced to reflect the fact that procrastination and temptation are opposites. Actual behavior may also be driven by individual differences because those with self-insight will be aware that they are prone present bias but will be sophisticated enough to realise that this might generate inconsistent behavior [64]. They will rationally decide to set up precommitment devices to moderate the impact of future temptations. In the context of security and privacy problems, they can be encouraged to setup precommitment devices such as identity verification systems or setting computer default options which exploit the status quo bias so that they are effectively making less effort to protect themselves from security violations in the future.

Habits will also play a role and models of habit formation can be developed from insights about adjacent complementarity [19]: utility in the past and present is complementary to utility in the present and future which means that habits will persist over time; so if sensible habits to protect privacy and security can be inculcated then over time these habits will become more and more ingrained. If people can be encouraged to repeat good habits (e.g. backing-up files, doing regular virus checks) often enough then the habits will stick and people will do more to protect their online privacy and security

4 Empirical Analysis

In the preceding section, some of the behavioural constraints on the management of online privacy and security were outlined and in this section, survey data from the 2009/10 British Crime Survey is used to analyse some real-world behavioural patterns.

4.1 Empirical hypotheses

The following empirical hypotheses will be explored:

Hypothesis 1 *Individual differences, e.g. differences in age, gender and socioeconomic background, will explain an individual's susceptibility to fraud.*

Hypothesis 2 *Susceptibility to fraud will also be affected by behavioural differences and victims are more likely to be regular users of the internet and specifically of online banking and shopping.*

Hypothesis 3 *Precautionary behavior (e.g. shredding documents, changing PINs, taking out anti-fraud insurance) will vary across individuals and will be affected by demographic differences in age, gender and socioeconomic background.*

Hypothesis 4 *Precautionary behavior will also be affected by behavioural differences with regular internet users being more experienced and better informed and therefore more likely to take precautions against fraud, particularly ”virtual” precautions, e.g. using computer security.*

Hypothesis 5 *Fraud victims are less likely to have taken precautions before fraud took place, i.e. were more vulnerable to fraud before it happened.*

Hypothesis 6 *Behavioural constraints will affect precautionary behavior and behavioural change amongst fraud victims after they were victims will be limited - reflecting procrastination, habit persistence and/or slow learning.*

Hypothesis 7 *These behavioural constraints will be balanced by the magnitude of financial losses and those who suffered large financial losses as a result of fraud are less likely to procrastinate and will be more likely to take precautions after fraud takes place.*

Hypothesis 8 *Psychological factors will play a role and people with strong emotional reactions to the threat of fraud will be less likely to behave in a substantively rational way and therefore will be no more likely to take precautions than those who don't have a strong emotional response to the threat of fraud.*

4.2 Data sources

These empirical hypotheses will be explored using STATA to analyse data from the 2009/10 British Crime Survey (BCS). BCS participants are asked a wide range of questions about their experience of and attitudes towards crime. Recent versions of the survey have included questions about fraud /identity theft, level and type of internet use, nature of anti-fraud precautions employed as well as a collection of demographic questions. The specific details and definitions of the variables used in the empirical analysis are summarized in Appendix 1. Most of the variables are self-explanatory with the exception of the sets of BCS questions about precautions taken against fraud. To enable parsimonious estimation, these questions have been amalgamated into broad measures as follows: whether or not physical precautions, e.g. shredding documents, checking cash-points etc, have been used; whether or not virtual precautions, including regularly changing PINs, using only secure websites and using security software, have been used; and whether or not insurance was taken out. Respondents were asked to indicate whether or not they are taking these precautions now and, where applicable, whether they took them *before* they were defrauded. This enables an analysis of behavioural change, as explored below.

4.3 Likelihood of fraud

The probability that a respondent had suffered bank fraud via use of their personal details without permission was estimated using a probit link function to capture the impact of internet use, demographic characteristics and precautionary behaviour on the probability of fraud. The results from the estimation are outlined in Table 1 and show that people who use online banking are more vulnerable to fraud, people in higher socio-economic groups are more vulnerable to fraud and people who take physical precautions are less vulnerable to fraud. Virtual precautions have no significant impact on the probability that a person has experienced fraud.

Table 1: **Risk of fraud**
Probit estimation with robust standard errors n=14,260

Regressor	Parameter estimate	t ratio	p value
Internet use	-0.016	-0.600	0.549
Online banking	0.183	3.580***	0.000
Online shopping	0.066	1.190	0.234
Online social networking	0.022	0.460	0.649
Gender	0.037	0.850	0.393
Age	0.000	-0.900	0.368
Socioeconomic group	-0.037	-3.450***	0.001
Virtual precautions	0.018	0.550	0.586
Physical precautions	-0.049	-3.750***	0.000
Insurance	0.030	0.610	0.541
Constant	-1.745	-14.640	0.000***
n=14,260			
Likelihood ratio test:			
$\chi^2(10) = 62.65$ $[p = 0.000]$			

4.4 Precautionary habits

To establish what factors are associated with precautionary behaviour, three models were estimated using either Tobit for censored regressions (for the estimations of number of virtual versus physical precautions taken) and probit for the binary dependent variable capturing whether or not people took out insurance against fraud. As explained above, the BCS provides data on precautions taken before fraud and after fraud so these models incorporate the before fraud behaviour as an explanatory variable and the parameter estimate on this variable will show the persistence of habits and/or the degree of learning. Other regressors included in the precautionary measures estimations include whether or not someone has been a victim of fraud, their emotional responses / extent of worry about card fraud, levels of internet use including online banking, online shopping and online social networking and demographic variables, The results are outlined in Tables 2 to 4.

The results from the estimation of virtual precautions (see Table 2) indicate that fraud victims are less likely to take virtual precautions against fraud suggesting that they are not learning from their exposure to fraud and are not changing the precautions they take in response to their experiences. Further estimations of changes in virtual precautions (not reported here) showed that there is no significant relationship between increasing virtual protections and the magnitude of reported losses from fraud. In addition there is a strong degree of persistence with an almost one-to-one relationship between precautions taken before and after fraud. This again suggests that any learning about the value of taking precautions is limited and/or habits are sticky / persistent and so if someone is not in the habit, e.g. of changing their PINs, then their precautionary behaviour is unlikely to change even if they are a victim of fraud. The results from the estimation of physical precautions (see Table 3) confirm the stickiness and persistence of habits and again the parameter estimate on precautionary behaviour before fraud

Table 2: **Virtual precautions against fraud**

Tobit estimation

Regressor	Parameter estimate	t ratio	p value
Virtual precautions before	1.056	59.020***	0.000
Fraud victim	-0.072	-2.560**	0.011
Emotional response (1=high)	-0.007	-0.330	0.738
Card worries (1=high)	0.024	1.380	0.169
Internet use	-0.013	-0.650	0.513
Online banking	0.080	2.510**	0.012
Online shopping	0.002	0.040	0.967
Online social networking	0.020	0.710	0.477
Gender	0.029	1.090	0.278
Age	0.000	-0.640	0.525
Socioeconomic group	-0.004	-0.670	0.506
Constant	-0.267	-2.920***	0.004

n=1275

Likelihood ratio test:

$\chi^2(11) = 2066.84 \ \ [p = 0.000]$

Table 3: **Physical precautions against fraud**

Tobit estimation

Regressor	Parameter estimate	t ratio	p value
Physical precautions before	0.944	72.730***	0.000
Fraud victim dummy	0.034	0.600	0.546
Emotional response (1=high)	-0.106	-2.700***	0.007
Card worries (1=high)	0.011	0.320	0.750
Internet use	0.067	1.850*	0.065
Online banking	0.031	0.510	0.610
Online shopping	-0.002	-0.030	0.977
Online social networking	0.075	1.350	0.178
Gender	0.020	0.380	0.705
Age	0.000	-0.100	0.917
Socioeconomic group	-0.012	-0.900	0.370
Constant	0.380	2.100**	0.036

n=1275

Likelihood ratio test:

$\chi^2(11) = 2149.21 \ \ [p = 0.000]$

is approximately equal to one. In addition, a heightened emotional response (in the BCS high emotions are given a low numerical value) are associated with more physical precautions which may be explained by the fact that heightened emotion is propelling precautionary beahviour. More regular internet use is associated with more physical precautions, perhaps because regular internet users are more aware of the dangers to which they re explosed. Fraud victims are not significantly more or less likely to protect themselves after fraud. In addition there is a strong degree of persistence with an almost one-to-one relationship between precautions taken before and after fraud and, as for virtual precautions, this suggests that any learning about the value of taking precautions is limited and/or habits are sticky / persistent.

Table 4: **Insurance against fraud**

Probit estimation

Regressor	Parameter estimate	t ratio	p value
Insurance before	3.893	23.290***	0.000
Fraud victim dummy	-0.150	-0.930	0.351
Emotional response (1=high)	-0.201	-1.720*	0.085
Card worries (1=high)	-0.016	-0.160	0.875
Internet use	-0.140	-1.410	0.160
Online banking	0.096	0.500	0.618
Online shopping	-0.224	-1.020	0.307
Online social networking	0.067	0.370	0.709
Gender	-0.179	-1.110	0.265
Age	-0.001	-0.250	0.800
Socioeconomic group	0.000	0.000	0.996
Constant	-1.024	-1.790*	0.074

n=1275

Likelihood ratio test:

$\chi^2 11) = 1228.32$ [$p = 0.000$]

The results from the probit estimations of decisions to insure (see Table 4) show again that precautionary measures are persistent suggesting slow learning and/or sticky habits. Apart from that, the only significant parameter is that on emotional response and this is similar to the response for physical precautions: less emotion (higher scores on the emotional response variable) is associated with a lower probability of insurance and, as for physical precautions, fear of fraud may propelling the decision to insure.

4.5 Discussion of results

The results above suggest that certain features are associated with different aspects of fraud risk and precautionary behavior. People who use online banking are more susceptible to fraud which is unsurprising as they probably are more exposed to attack. Those in higher socioeconomic groups are more vulnerable to fraud, perhaps because they have greater access to financial services and/or have sufficient income and wealth to attract frausters. The factors associated with precautionary behavior vary between those who use more virtual precautions (e.g. identifying safe websites from padlock symbol, regularly changing PINs and using computer security measures) versus those who use more physical precautions; but in both categories, the significance of the lagged precautions variables for all empirical models of precautionary behaviour suggest that there is strong persistence in behavior suggesting that procrastination, slow learning and/or sticky habits affect behaviour. For virtual precuations, the other significant factors are that more worry is associated with fewer precautions (though the direction of causality is unclear) and those use online banking are more likely to use virtual precautions. People who have previously been fraud victims are less likely to use virtual precautions suggesting that learning is slow, that fraud victims are more likely to procrastinate about setting up protections and/or that habits dominate and are unlikely to change.

5 Conclusions and Policy Implications

In designing effective policies to ensure privacy and enhance security a key policy debate focuses on the relative roles to be played by government regulation versus private initiative. In designing mechanisms to ensure that people adopt a more responsible approach to protecting themselves online, policies will need to take account of the realities of human behaviour by keeping the alternative options simple and cheap. Also, given rapid technical change e.g. in the growth of cloud computing and mobile technologies, policy solutions must also be flexible and adaptable to changes in people's computing habits. Since 911, geopolitical factors have necessitated a cautious approach to the development of systems especially those which enable the cheap and anonymous electronic movement of money. For phishing attacks, the marginal costs are very low for the perpetrators and the chances of being caught are slim so a significant problem will be formulating strategy proof designs given the very small costs faced by perpetrators. Is it ever going to be possible to manipulate their incentives to prevent privacy and security violations? Fines and penalties might be more effective but, for both phishing and online fraud, the capacity for governments effectively to police these violations is limited. So effective solutions will necessarily have to concentrate on encouraging people to take a longer term view when protecting their privacy and security. Sophisticates who are well-informed about the dangers of identity theft etc. may use pre-commitment devices without much prompting but for people who have limited knowledge or experience, psychological and emotional factors will exert significant impacts and so policies should be designed to take account of these subjective factors as well as objective ones.

6 Data Appendix

Data codes and definitions are outlined in Table 5. Data are from the 2009/10 British Crime Survey, accessed via the UK Data Archive. Material from Crown copyright records made available through the Home Office and the UK Data Archive has been used by permission of the Controller of Her Majesty's Stationery Office and the Queen's Printer for Scotland (Usage No 5571). Those who carried out the original analysis and collection of the data bear no responsibility for the further analysis and interpretation of these data in this paper. In submission to the Home Office for comment before distribution.

Table 5: **British Crime Survey (BCS) Data Codes, Questions and Definitions**

Variable	Code	Definition
Fraud victim	qbnkuse	Have personal details been used fraudulently?
Loss	qloss2	Range of monetary loss?From 0 to ¿1000
Emotional response	qfremot	How emotionally affected? 1=Very,3=Little
Card worries	qcardw	How worried are you about card fraud?
Precautions before	qpreca-s	Was precaution taken before fraud?
Precautions now	qprec2a-s	Is precaution taken nowadays?
Internet use	intern2	Internet use 1=used daily 7=used every 3 months or less
Online banking	intern3a	Do you use the internet for online banking?
Online shopping	intern3a	Do you use the internet for online shopping?
Online social networking	intern3i	Do you use the internet for social networking?
Gender	sex	1=Male, 2=Female
Age	age	Numeric value
Socioeconomic group	respsec2	Socioeconomic Classification,1=professional,8=never worked

References

[1] Acemoglu D 1992, Learning about others' actions and the investment accelerator *Economic Journal* vol 103, no 417, pp 318-28.

[2] Acquisti A 2004, Privacy in Electronic Commerce and the Economics of Immediate Gratification, EC 2004.

[3] Acquisti A and Grossklags J 2006, What can behavioral economics teach us about privacy, ETRICS 2006.

[4] Afzal S and Robinson P, Modelling Affect in Learning Environments: Motivation and Methods.

[5] Afzal S and Robinson P 2009, Natural Affect Data: Collection and Annotation in a Learning Context, IEEE 2009.

[6] Akerlof G 1970, The Market for Lemons: Quality Uncertainty and the Market Mechanism *Quarterly Journal of Economics* vol 84, no 3, pp 488-500.

[7] Akerlof G and Shiller R 2009, *Animal Spirits: How Human Psychology Drives the Economy and Why it Matters for Global Capitalism* Princeton, Princeton University Press.

[8] Anderson R 2011, Security and Human Behavior Conference 2011, Carnegie Mellon.

[9] Anderson J L 1998, Embracing uncertainty: the influence of Bayesian statistics and cognitive psychology, *Conservation Ecology* vol 2, no 1.

[10] Anderson R, Moore T 2008, Information Security Economics and Beyond, Information Security Summit 2008.

[11] Anderson R, Moore T 2009, Information security: where computer science, economics and psychology meet, *Philosophical Transactions of the Royal Society A* vol 367, pp 2717-2727.

[12] Angeletos G, Laibson D, Repetto A, Tobacman J and Weinberg S 2001, The Hyperbolic Consumption Model: Calibration, Simulation, and Empirical Evaluation *Journal of Economic Perspectives* Vol 15, no 3, pp 47-68.

[13] Axelrod R 1984 *The Evolution of Cooperation* Harmondsworth UK, Penguin.

[14] Baddeley M 2004, Using ecash in the New Economy: An economic analysis of micropayments systems *Journal of Electronic Commerce Research*, vol 5, no 4, pp 239-53.

[15] Baddeley M 2006, Behind the Black Box: a survey of realworld investment appraisal approaches *Empirica*, vol 33, no 5, pp 329-350.

[16] Baddeley M 2010, Herding, Social Influence and Economic Decision-Making: SocioPsychological and Neuroscientific Analyses, *Philosophical Transactions of the Royal Society B*, vol 365, no 1538, pp 281-290.

[17] Baddeley M, Curtis A and Wood R 2005, An introduction to prior information derived from probabilistic judgments: elicitation of knowledge, cognitive bias and herding, *Geological Prior Information: Informing Science and Engineering* edited by A Curtis and R Wood, Geological Society, London, Special Publications No 239, pp 15-27.

[18] Banerjee A 1992, A Simple Model of Herd Behavior, *Quarterly Journal of Economics*, vol 107, no 3, pp 797-817.

[19] Becker G S and Murphy K M 1988, A theory of rational addiction of Political Economy vol 96(4): 675-700.

[20] Bernheim BD and Rangel A 2004, Addiction and Cue-Triggered Decision Processes Economic Review, vol 94(5): 1558-90.

[21] Bikhchandani S, Hirshleifer D and Welch I 1992, A theory of fads, fashions, custom and cultural change as informational cascades, *Journal of Political Economy*, vol 100, no 5, pp 992-1026.

[22] Bikhchandani S, Hirshleifer D and Welch I 1998, Learning from the Behavior of Others: Conformity, Fads, and Informational Cascades, *Journal of Economic Perspectives*, Vol 12, No 3, pp 151-170.

[23] Basili M and Zappia C 2009, Shackle And Modern Decision Theory, *Metroeconomica*, vol 60, no 2, pp 245-282.

[24] Beresford A R, Kubler D, and Preibusch S 2010, Unwillingness to pay for privacy: a field experiment, *IZA Discussion Papers*, IZA DP5017, Institute for the Study of Labor, Bonn.

[25] Blackmore S 1999, *The Meme Machine*, Oxford, Oxford University Press.

[26] Bliss JP, Gilson RD and Deaton JE 1995, Human probability matching behaviour in response to alarms of varying reliability, *Ergonomics*, vol 38, pp 2300-2312.

[27] Bonneau J and Preibusch S 2009, The Privacy Jungle: On the market for Data Protection in Social Networks, WEIS 2009.

[28] Brunnermeier M 2001, *Asset pricing under asymmetric information*, Oxford, Oxford University Press.

[29] Bulmer M G 1979, *Principles of Statistics*, New York, Dover.

[30] Chamley C P 2003, *Rational herds economic models of social learning*, Cambridge, Cambridge University Press.

[31] Clark 2010, A social embedding of network security: trust,constraint, power and control, Security and Human Behaviour 2010.

[32] Cranor L 2011, Security and Human Behavior Conference 2011, Carnegie Mellon.

[33] Davidson P 1991, Is Probability Theory Relevant for Uncertainty? A Post Keynesian Perspective, *Journal of Economic Perspectives*, vol 5, pp 129-143.

[34] Dawkins R 1976, *The Selfish Gene*, Oxford, Oxford University Press.

[35] DellaVigna S and Malmendier U 2006, Paying Not to Go to the Gym *American Economic Review* vol 96, no 3, pp 694-719.

[36] Economides N 1996, The Economics of Networks, *International Journal of industrial Organisation* vol 14, no 6, pp 673-99.

[37] Eichenberger 2001, Economic incentives transform psychological anomalies, in Feltovich F J, Ford K M and Hoffman R R *Expertise in Context: Human and Machine*, Cambridge MA: MIT Press, pp 21-36.

[38] Elster J 1996, Rationality and the emotions, *Economic Journal*, vol 106, no 438, pp 136-197.

[39] Elster J 1998, Emotions and economic theory, *Journal of Economic Literature*, vol 36, no 1, pp 47-74.

[40] Erev I and Roth A 1998, Predicting how people play games: Reinforcement learning in experimental games with unique, mixed-strategy equilibria, Economic Review, vol 88(4):848881.

[41] Evans D 2011, Security and Human Behavior Conference 2011, Carnegie Mellon.

[42] Frederick S, Lowenstein G and O'Donoghue T 2002, Time Discounting: A Critical Review, *Journal of Economic Literature*, vol 40, no 2, pp 351-401.

[43] Gul F and Pesendorfer W 2001, Temptation and Self Control, *Econometrica*, vol 69(6):1403-1435.

[44] Laibson, D 1997, Golden eggs and hyperbolic discounting, *Quarterly Journal of Economics* vol 112, pp 443-477.

[45] Gigerezner G 2007, *Gut Feelings*, London, Allen Lane.

[46] Gigerezner G and Goldstein DG 1996, Reasoning in a fast and frugal way: models of bounded rationality, *Psychological Review*, vol 103, pp 650-669.

[47] Hirshleifer J 1983, From weakest link to best shot: the voluntary provision of public goods, *Public Choice*, vol 41, no 3, pp 371-386.

[48] Gould P 1970, Is *Statistix inferens* the geological name for wild goose. *Economic Geography* vol 46, pp 438-448.

[49] Kahneman D and Tversky A 1973, On the psychology of prediction, *Psychological Review*, vol 80, pp 237-51.

[50] Kahneman D and Tversky A 1979, Prospect Theory: An Analysis of Decision under Risk, *Econometrica*, vol 47, no 2, pp 263?292.

[51] Katz M L and Shapiro C (1994) Systems Competition and Network Effects, *Journal of Economic Perspectives*, vol 8, no 2, pp 93-115.

[52] Kennedy P 1998, *Guide to Econometrics*, Oxford, Blackwell.

[53] Keynes J M 1921, *A Treatise on Probability*, Macmillan, London.

[54] Keynes J M 1930, *Treatise on Money*, Macmillan, London.

[55] Keynes J M 1936, *The General Theory of Employment, Interest and Money*, Macmillan, London.

[56] Keynes J M 1937, The General Theory Of Employment, *Quarterly Journal of Economics*, vol 51, pp 209-223.

[57] Kyland F E and Prescott C E 1977, Rules rather than discretion: the inconsistency of optimal plans, *Journal of Political Economy* Vol 85, No 3, pp 473-492.

[58] Kyberg H E 1997, Expertise and context in uncertain inference, in Feltovich F J, Ford K M and Hoffman R R *Expertise in Context - Human and Machine*, Cambridge MA: MIT Press, pp 499-514.

[59] Lo A W 2001, Bubble, rubble, finance in trouble? Edited luncheon address, 3rd Annual Institute of Psychology and Markets Conference, New York City, June 2001.

[60] Lynch A 1996, *Thought Contagion: How Belief Spreads Through Society*, New York, Basic Books.

[61] Lynch A 2003, An introduction to the evolutionary epidemiology of ideas, *The Biological Physicist*, vol 3, pp 7-14.

[62] Minksy M 1997, Negative expertise, in Feltovich F J, Ford K M and Hoffman R R *Expertise in Context: Human and Machine*, Cambridge MA: MIT Press, pp 515-521.

[63] Odlyzko A 2003, Economics, Psychology, and the Sociology of Security, *Financial Cryptography 2003.*

[64] O'Donoghue T and Rabin M 1999, Doing It Now or Later, *American Economic Review*, vol 89, no 1, pp 103-24.

[65] O'Donoghue T and Rabin M 2001, Choice and Procrastination, *Quarterly Journal of Economics*, vol 116, no 1, pp 121-160.

[66] The Mirror System In Humans, in Stamenov M I and Gallese V (eds) *Mirror Neurons And The Evolution Of Brain And Language: Advances In Consciousness Research*, vol 42, Amsterdam, John Benjamins, pp 37-59.

[67] Shackle G L S 1953, The logic of surprise, *Economica*, vol 20, pp 112-117.

[68] Shapiro C and Varian H R 1998, *Information Rules: A Strategic Guide to the Network Economy* Massachusetts, Harvard Business School Press.

[69] Scharfstein D S and Stein J C 1990, Herd behaviour and investment, *American Economic Review*, vol 80, no 3, pp 465-79.

[70] Schultz W 2006, Behavioral theories and the neurophysiology of reward, *Annual Review of Psychology*, vol 57, pp 87-115.

[71] Shiller R J 1995, Conversation, Information and Herd Behavior, *American Economic Review*, vol 85, no 2, pp 181-85.

[72] Shiller R J 2000, *Irrational exuberance*, Princeton, Princeton University Press.

[73] Shiller R J 2003, From Efficient Markets Theory to Behavioral Finance, *Journal of Economic Perspectives*, vol 17, no 1, pp 83-104.

[74] Shulz P, Nolan J, Cialdini R, Goldstein N and Griskevicius V 2007, The constructive, destructive and reconstructive power of social norms, *Psychological Science*, vol 18, pp 429-34.

[75] Schwarz N 2000, Emotion, cognition and decisionmaking, *Cognition and Emotion*, vol 14, pp 433-440.

[76] Shy O 2001, *The Economics of Network Industries*, Cambridge, Cambridge University Press.

[77] Simon H 1979, From substantive to procedural rationality, in F H Hahn and M Hollis (eds), *Philosophy and Economic Theory*, Oxford, Oxford University Press.

[78] Skinner D C 1999, *Introduction to Decision Analysis*, Delaware, Probabilistic Publishing.

[79] Slovic P, Finucane M, Peters E and MacGregor DG 2004, Risk as analysis and risk as feelings: some thoughts about affect, reason, risk, and rationality, *Risk Analysis* vol 24(2): 311-322.

[80] Sornette D 2003, *Why Stock Markets Crash: Critical Events in Complex Financial Systems*, Princeton, Princeton University Press.

[81] Thaler R H and Sunstein C 1999, Mental Accounting Matters, *Journal of Behavioral Decision Making*, vol 12, no 3, pp 183-206.

[82] Thaler R and Sunstein C 2008, *Nudge: Improving Decisions about Health, Wealth and Happiness* Yale: Yale University Press.

[83] Topol R 1991, Bubbles and volatility of stock prices: effect of mimetic contagion, *Economic Journal*, vol 101, no 407, pp 786-800.

[84] Tversky A and Kahneman D 1974, Judgement under uncertainty: heuristics and biases, *Science*, vol 185, 1124-1131.

[85] Tversky A and Kahneman D 1982. Judgements of and by representativeness, in Kahneman D, Slovic P and Tversky A (eds) *Judgement under Uncertainty: heuristics and biases*, Cambridge, Cambridge University Press, pp 84-98.

[86] Varian H 2004, *Intermediate Microeconomics*, Norton Publishing.