

Information Security: Lessons from Behavioural Economics

Michelle Baddeley

Gonville and Caius College, University of Cambridge, UK *

June 2011

Abstract

Psychological and sociological factors constrain economic decision-making in many contexts including the online world. In particular, uncertainty limits the optimising behaviour which is often the focus of economic models and so people will be forced to rely on simpler decision-making rules when managing information online. Behavioural economics and economic psychology emphasise that people will make many mistakes in processing information and planning for the future and these mistakes will also distort learning processes. Emotions and visceral factors will play a key role - not only affecting people's actions and choices but also the connection between information, learning and choices. All these forces will have wide-ranging implications for information security management and this paper summarises some of the key insights and policy lessons for information security.

Keywords: behavioural economics, information security, cognitive bias, present bias, emotional processing

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 electronic spending. Electronic solutions including electronic cash and mobile payments are proving to be potentially superior substitutes for conventional monetary instruments but significant problems have emerged because alongside the positive innovations, significant abuses have grown concomitantly, including not only anti-social behaviour and security/privacy abuses such as spam attacks, phishing and identity theft but also vulnerability to online exploitation e.g. via online payday loan companies. Whilst there are technical dimensions and solutions to these problems, the most effective solutions will have to address the realities of real-world human behaviour, raising some crucial policy

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

questions. To what extent should governments intervene to prevent these abuses? To what extent are individuals able to control for themselves the personal and financial information that they release to the world via email and the internet? To inform our understanding specifically about what individuals can do to protect themselves in a computerised world this paper outlines a series of insights from economics in general and behavioural economics in particular.

2 Economic models of rational choice

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 model of human decision-making which is clear and simple, it often lacks realism and empirical validity. This approach assumes markets and behaviour which are perfect, on average at least, and it is difficult fully to understand within such a stark approach the full 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 Externalities and network effects

In understanding the links between computer security and human behaviour, it is important to focus on some particular features of 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, and also because of other distinctive but related characteristics of networked goods including complementarities, externalities and switching costs [43], [68], [31]. Furthermore, given heterogeneity of preferences and shifting preferences, profits can be made from price discrimination. There are commercial incentives to erode privacy in order to target different groups in different ways [9], [10]. 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. 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. In an online context for example, the additional value for an individual of signing up to an electronic payment system will be small if other consumers are not using the same pay-

ment system [43], [31]. In a dynamic context, this means that multiple equilibria can exist in which a producer will 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. For electronic payment networks to grow, ensuring widening acceptability is crucial and, in theory at least, acceptability of a system should be affected by the efforts it makes to secure privacy. 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 [24]. 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. 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 [21]. Switching costs and lock-in may apply if exiting a payment system is relatively more costly than entering it [60]. 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. Finally, economies of scale will mean that whilst there are high sunk or fixed costs involved 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 payment system producers if the costs of developing new privacy and security infrastructure have to be borne by private institutions.

2.2 Security as a public good

Network externalities are also linked to the fact that security is a quasi public good. From consumers' point-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 problem: consumers are able to free ride on the benefits of others' cautiousness without incurring any of the costs, generating a Prisoner's Dilemma type game [9] [10].

2.3 Imperfect information and misaligned incentives

Standard economic models can be adapted to incorporate the market failures associated with imperfect information and misaligned incentives. For example, adverse selection is a pre-contractual problem in which a product's attributes is hidden information. 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. 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 [10]. Asymmetric information also leads to a post-contractual principal agent problems of moral hazard, i.e. hidden action. Principal-agent problems lead to inefficiencies when the incentives of a principal and agent are different and, with moral hazard, the principal cannot effectively monitor the efforts of their agent. For example, 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 any area involving team effort. 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 [10] [77] [39]. 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 members of the online "team" 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; the implication for security systems is that they become particularly vulnerable to attack.

3 Bounded rationality

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 happens in a world of uncertainty and imperfect information. Limits on rationality are likely to be profound if the world is mutable and economic reality reflects endogenous processes. In this case, a consistent, immutable and objec-

tive reality may be missing; reality will be changing as expectations change. These models by definition neglect socio-psychological forces affecting security and human behaviour, though the gap between the two can be bridged to an extent by approaches which recognise the constraints on rational choice in a world of risk, uncertainty and imperfect information. Importantly and significantly Herbert Simon softened economists' conceptions of rationality by introducing models of bounded rationality and distinguishing substantive rationality from procedural rationality [69] [14]. Bounded rationality occurs when individuals' rationality is constrained by imperfect information, cognitive limitations, and time pressures. If people are boundedly rational then the sensible application of clear and objective mathematical rules will be impossible because the existence of immeasurable uncertainty precludes the quantification of probabilities of future events. Bounds to rationality can be understood in terms of Simon's distinction between substantive rationality and procedural rationality. Simon defines substantive rationality as occurring when people focus on the achievement of objective goals given constraints [69]. If people are substantively rational, then they will form quantifiable expectations of the future and will make their decisions using constrained optimisation techniques to balance marginal benefits with costs and maximise utility. They will use mathematical algorithms to guide their decisions. This implies that, 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 (ie discount rate) into their decision-making process. By contrast, procedurally rational behaviour is based on a broad reasoning process rather than the achievement of given representative agent's goals [69]. 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.

3.1 Substantive rationality

A particular problem for models of behaviour based on substantive rationality lies in capturing how people deal with risk and uncertainty when making choices that have future consequences. In using the internet and in particular when using an online payments system or a 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. In either the substantive or the procedural approach, some assumption or hypothesis must be formed to explain how people form their expectations about the future. Prediction is particularly complex when it comes to economic processes because the economic world is changeable: peoples' beliefs about economic structure have the capacity to change that economic structure, as emphasised in the mainstream macroeconomic literature on dynamic inconsistency [49] and the heterodox literature on non-ergodicity [28]. This suggests that Classical statistical or 'frequentist' approaches to the analysis of probability which assume repeatable events, complete information and/or an understanding of the data-generating mechanism, will be of little use in understanding the predictions of fixed asset investors for three reasons. First, information is incomplete and the datagenerating processes dictating economic outcomes are often unknown. Secondly, many human decisions are

about nonrepeatable, unprecedented events and this means that information about past outcomes will be of little use. Thirdly, endogeneity and circularity mean that economic realities are complex and mutable. 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. 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. Given these three sources of complexity, the objective basis for probabilistic judgements may be missing or unknowable and the third source of complexity will undermine even more subjectively based Bayesian probability concepts. The overall lesson is a model incorporating an assumption of substantive rationality is unlikely fully to capture the realities of human behaviour in the context of computer security decisions.

3.1.1 Risk, uncertainty and limits to quantification

In understanding how people form expectations, the basic distinction common to several frameworks of probability and uncertainty found in different academic disciplines is that between different probability concepts *viz.* objective probability versus subjective / inductive probability and between relative frequencies of events verifiable via observation and experiment versus opinions and beliefs [26]. Paralleling subjective probabilities, inductive probabilities act as a guide to life and are formed even when an anticipated event is unprecedented; they therefore have no necessary association with frequency ratios. They are not based on *ex ante* prediction; they are formed in the face of uncertainty and incomplete knowledge yet, in most areas of academic investigation, inductive probabilities are of greater practical importance than statistical probabilities because knowledge of an underlying objective reality is either limited or absent. With incomplete knowledge, statistical probabilities based upon past outcomes and an assumption of stationarity, are often inappropriate to the analysis of people's judgements in complex situations. These distinctions mirror Keynes's distinctions between Knightian risk (the quantifiable risks associated with frequentist concepts) and Knightian uncertainty - which is unquantifiable [45]. 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 have more common than those characterised by Knightian risk, at least in the economic and social sphere. Such issues are of particular importance in economics because much economic behaviour is forward looking, experiments may not be repeatable, and conditions cannot be controlled. People often make subjective probability judgements about events that have not occurred before, for which the data generating mechanism cannot be known. This makes the quantification and assessment of probabilities particularly problematic because it becomes impossible to match subjective probability judgements with an objective probability distribution. Also, endogeneity (i.e. the path a system takes is determined by events within the system) will limit the accuracy of probabilistic judgements of future events when beliefs about the future are affected by beliefs about the present. Errors in expectations will be non-random and will not cancel out. Instead they may spread

generating systematic trends. Shiller analyses such phenomena in the context of feedback theory, describing the endogeneity in belief formation: beliefs about the system determine the path of that system e.g. stock prices go up because people believe they will go up [63], [64], [65]. The differences between these probability concepts can be reconciled, to an extent, using a Bayesian model of economic decision-making. There are, however, 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 [44]. 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 [55]. Human intuitive cognitive processes do not deal well with more flexible Bayesian thinking methods either. In the context of security and human behaviour, online decision-making is more likely to be governed by subjective / inductive probabilities: 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 [9] [10]. But for decisions relating to internet use for example, 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 Procedural rationality and cognitive limits

As noted above, Simon (1979) argues that economic decisions are more often the product of a 'procedurally rational' process rather than substantive rationality. The behaviour of the procedurally rational person does not involve constrained optimisation. Instead, people will be guided by "appropriate deliberation" i.e. doing the best that they can, given the circumstances. A procedurally rational person will use common sense rather than complex mathematical techniques in assessing their current and future choices. In contrast to the substantive approach, this implies that different people, even if they are using the same information, will form different expectations reflecting arbitrarily assigned margins of error. In an uncertain world, actual experience will be surprising by comparison with expectations because an imperfect image has been formed in advance (Shackle 1953, Basili and Zappia 2009) [59], [20]. If people are procedurally rational and the logical link between objective and subjective probabilities is broken, then a range of choices may be defensible. But if these 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 [76] [16]. 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.

3.2.1 Cognitive bias and heuristics

Following from above, research on prospect theory shows that the standard approach to subjective utility has many limitations [42]. Also it is consistent with the fact that most ordinary people make common mistakes in their judgements of probabilities (e.g. Anderson 1998) generating individual and group biases [16]. This links into bounded rationality because it reflects limits on the processing ability of the human mind [40] [75] [8]. 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 [70]. 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. Overconfidence is especially a problem for extreme probabilities which people tend to find hard to assess, which will be relevant for computing decisions and in the absence of meaningful and available information about security threats, people will be overly sanguine, for example about their vulnerability to identity theft. Many other cognitive biases have been identified too including status quo bias, attribution error, endowment effects and loss aversion. For security and human behaviour, 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] [73]. 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 be too lazy to change these options thus protecting them 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 will adopt the heuristic of following the crowd, i.e. buying what their friends are buying. At least four types of heuristics that produce cognitive bias are commonly employed: availabil-

ity, anchoring and adjustment, representativeness, and control [41] [75]. Availability 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. 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. On the other hand, 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. Other well-known biases introduced by the representativeness heuristic include the gambler's fallacy and base-rate neglect. The gambler's fallacy is the belief that when a series of trials have all had the same outcome then the opposite outcome is more likely to occur next time, since random fluctuations seem more representative of the sample space. Base-rate neglect involves discounting the relative frequency with which events occur and probability matching which occurs when reactions reflect the probabilities of the various consequences rather than the probability of the event itself and is used by humans and also some other primates [23]. World War Two bomber pilots provide an example: they were allowed to carry either a flak jacket or a parachute, but not both because of the extra weight. The pilots knew that getting strafed by enemy guns when a flak jacket would give best protection was three times more likely than being shot down when a parachute would be most useful. This is not an optimal assessment of the probabilities. Objectively, pilots were more likely to survive if they had flak jackets 100 per cent of the time because the probability of getting strafed by enemy guns was always more likely than the probability of being shot down - the flak jacket was always more likely to be of use. Yet the pilots were observed to take flak jackets three times out of every four and parachutes on the fourth occasions [51]. Anchoring and adjustment is a single heuristic that involves making an initial estimate of a probability called an anchor, and then revising or adjusting it up or down in the light of new information [75]. This typically results in assessments that are biased towards the anchor value. For example, in deciding about an appropriate wage demand to make, workers will anchor wage demands around their current wage. Anchoring effects may operate in a social dimension too if one individual's judgements is 'anchored' to others' opinions [75] [32]. 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. The control heuristic is the tendency of people to act as though they can influence a situation over which they have no control. If lottery ticket holders have chosen their own numbers rather than using random number selection then they will value their lottery tickets more highly even though the probability of a win is identical in both cases. The representativeness heuristic is where people use the similarity between two events to estimate the probability of one from the other [76]. The classic example is the "Linda problem". In experiments, a large proportion of people will judge it to be more likely that Linda is a social worker active in the feminist movement, than that she is an unspecified sort of social worker

even though the former is a subset of the latter and therefore is statistically equally or less probable. If this problem were to be expressed in probabilistic / statistical terms, anyone with a basic knowledge of probability would realise that two events happening together is less likely. However, when confronted with the details about Linda, most people find the first option more likely than the second, simply because they are influenced by the fact that way in which Linda is described by the experimenter to be more representative of a feminist stereotype. All these biases mean that people tend 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, again leading to an estimate of total probability in excess of one. So overall the estimated sum of all probabilities will be greater than one. Anderson argues that this is a consequence of the nature of memes, the cultural analogy of genes [8]. 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 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 in a situation in which it is not obvious that this is what is required, then they may make an instinctive, intuitive judgement which may generate statistical mistakes [50]. Anderson suggests that Bayesian approaches could be refined using the advantages of a frequentist approach by using mental, visual imagery and graphic display. In this way, some frequentist methods could be incorporated effectively into a Bayesian framework allowing human cognition to process subjective probabilities more effectively.

3.2.2 Present bias, time inconsistency and procrastination

Another type of decision-making bias that deserves particular attention is the present bias. People's behavior may be inconsistent over time: plans to do something constructive (e.g. backing-up files) in the future change as the future becomes the present because people procrastinate and they lack self control. This can be captured theoretically by a small tweak 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 [36] [11] [35] [73]. 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 using 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 it's a single lump sum and nothing if it 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 [72]. Acquisti and Grossklags have analysed the implications of present bias for people's choices about privacy and security [2] [3]. They also build on the behavioural economics literature on procrastination and self control [56], [57], [30].

When using the internet people will procrastinate about setting up effective security systems in much the same way as many ordinary 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. Assuming that people suffer present bias but are sophisticated enough to realise that this might generate security and privacy problems in the future, then 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 more effort to protect themselves from security violations in the shortterm. 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 forces such as gut feel. The term non-rational implies here that information is not being used in any systematic way. This does not necessarily imply that behaviour is stupid or misguided. The classic example is gut feel, a force that demonstrably drives entrepreneurs' decision-making [38], [37] [13]. Keynes's animal spirits - non-rational urges to act rather than remain idle - is a similar concept. Developing Keynes (1936), Akerlof and Shiller define animal spirits broadly, as the psychological factors affecting human behaviour [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). One of Akerlof and Shiller's animal spirits central to financial security is corruption: they argue that financial instability is exacerbated by the corruption that has grown during boom phases throughout history and this may have parallels for the online world because, as the internet and mobile networks grow, then the motives and opportunities for online crime will increase accordingly.

4 Learning and social influence

Standard economic models incorporate an assumption that people act as independent atomistic agents though modern economic theory does recognise that learning processes are important if people are only willing to search for information efficiently, i.e. will only search for more information when the marginal benefits exceed the marginal costs of that information. Behavioural economics has also explored the process of learning, building on insights from behaviourist psychology about conditioning; this led to the development of reinforcement learning models. Economists have also developed belief learning models focussed on the processes by which people learn about the beliefs 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 [74], [1]. Keynes argues that when your information is sparse you will do what others do because perhaps they know what they are doing [45], [46] [47] [48]. In Keynes's analysis, herding behaviours are linked back into an analysis of probabilistic judgement 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. Thus 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. This insight has been developed more recently by Sharfstein and Stein (1990), Banerjee (1992) and Bikhchandani, Hirschleifer and Welch amongst others [61], [17], [18], [19]. Social learning may also reflect broader social influences whether normative (e.g. peer pressure) or informational (e.g. learning from others' actions). 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 [64] [65] [74]citeBrunnermeier01 [71]. Whilst herding behaviour can be explained as a rational phenomenon, the existence of herding may still contribute to instability if the herd is led down the wrong path generating "herding externalities". Stable outcomes will only be achieved if the herd can be led along a path of increasing the stock of common (real) knowledge. In such cases, increases in the stock of reliable prior information will contribute to convergence in posterior probabilities. If, however, the herd path fosters increasing noise within the system then the process of opinion formation will become unstable. Lynch (1996, 2003) applies similar insights to the analysis of the evolutionary replication of ideas and argues that 'thought contagion' affects a wide range of human behaviours and beliefs [52], [53]. Social learning may interact with bias 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. Similarly, social influence can be described using evolutionary biological analogies, e.g. those based around the concept of memes - introduced above [29]. Imitation is a distinguishing characteristic of human behaviour and so a meme can be understood as a unit of imitation [22]. 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 [58]. 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 [8]. The implications for security and human behaviour are that if group leaders can be identified and encouraged to adopt appropriate online protections then others will follow their example. Alternatively, if information about the adoption of safeguards by others is prominent in information provided 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 [12]. The impact of social norms and social influence has been identified in the context of household energy choices [66] [73]. Similar influences may operate in the online environment too. In understanding these issues the roles of social capital, cooperation, trust and reputation are crucial. 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" [27]. Social norms affecting privacy and security are changing; 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, perhaps social norms can be manipulated in various ways including advertising, sanctions and rewards.

5 The role of emotions

Behavioural economics introduces a wide range of concepts and ideas with widespread implications for information security. One area that deserves particular attention is the role of emotional processing. The role of emotions is integral to economic decision-making [33],[34],[15]. This raises the conceptual question of whether or not behaviour is the outcome of irrational mistakes or procedurally rational devices. Are biases and heuristics procedurally rational but blunt decision-making tools i.e using information in a very rough way to cut costs and save time? Economists have traditionally been preoccupied by such distinctions between the rational and irrational but there is increasing recognition, particularly by some neuroeconomists, that this dichotomous approach is spurious. Neuroeconomics has a lot to offer in increasing our understanding of the neurological foundations of reward processing [62]. 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 lead to procrastination as discussed below. 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 and economic psychology. There will be three major steps via which people receive information, learn from that information and then make their decisions and emotions will affect the last two. Availability of information is constrained by asymmetric information, uncertainty and risk - these are the objective factors, at least to the extent that they will affect different people equally and will not be moderated by individual differences such as susceptibility to particular emotional states. In the second step of processing of information however, people will learn but their learning processes will be affected by cognitive limitations, including heuristics and biases, and emotional states will affect learning processes because they will impact on cognitive biases and heuristics. This is consistent with research that shows that psychological factors have particular significance because cognitive biases will be affected by emotional responses. People in a happy mood are more likely to use heuristics associated with topdown 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 [67]. In the third and final step, learning is translated into action; emotions and visceral factors will again have an impact because decisions will be the outcome of an interaction between reason and cognition versus emotion and affect. Minsky (1997) analyses emotional constraints arguing that the 'negative knowledge' associated with some emotional states may inhibit whole strategies of thought [54].

These three steps of information, learning and deciding and the constraints upon / interaction between them are captured in in Figure 1.

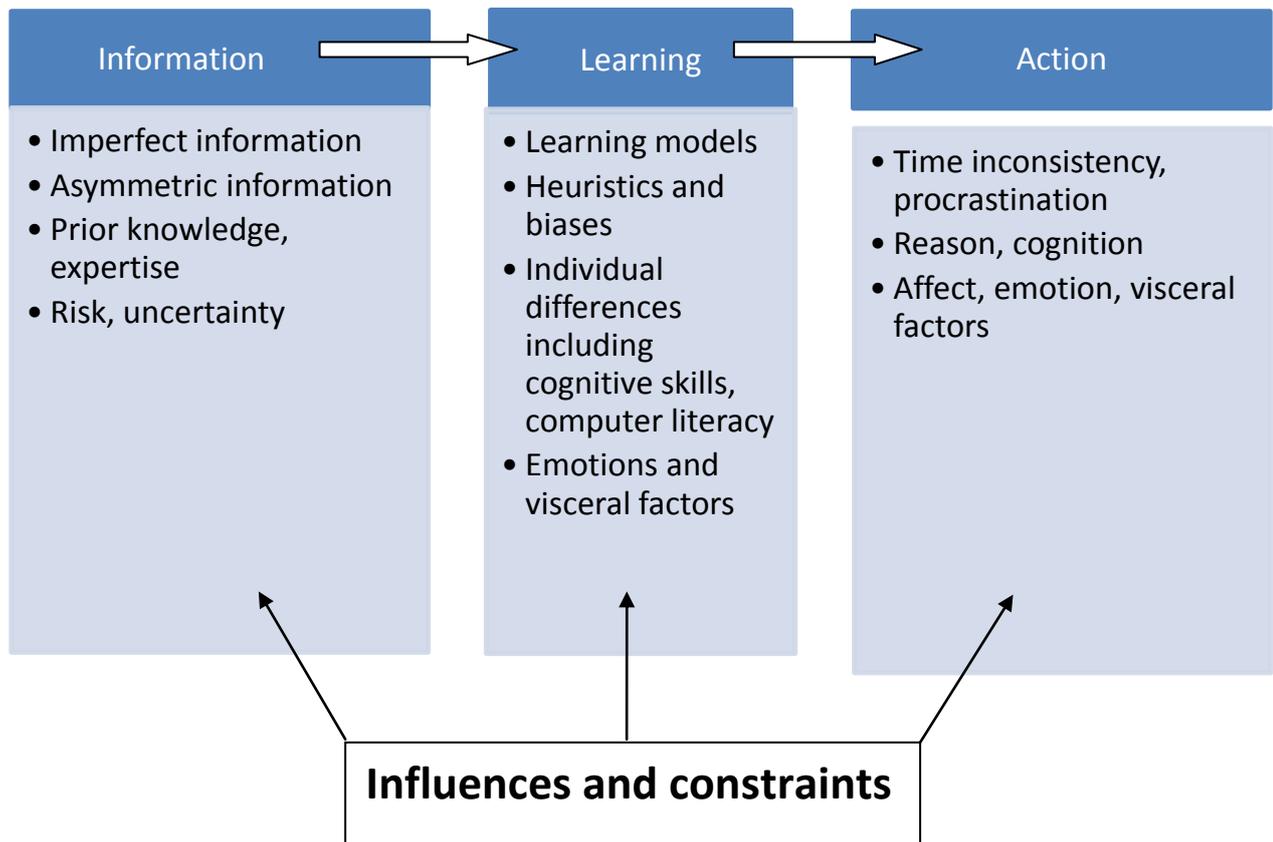


Figure 1: Stages of information gathering, learning and action

For computer privacy and security, learning is crucial because it determines how people adapt to innovative new technologies which may have many unfamiliar aspects. Personality will be an important variable affecting how individuals protect themselves and systems must be designed to suit different personality types [10]. Following from the insight that personality will also affect emotional responses, emotions have been shown to affect learning processes e.g. in computer based learning environments [4], [5].

6 Conclusions and policy implications

In designing effective policies to ensure privacy and enhance security a key policy debate is 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 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 spam and phishing? Fines and penalties might be more effective but, for both phishing and online fraud therefore, 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 more responsible attitude towards protecting their privacy. 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 the realities of human decision-making.

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 J L 1998, Embracing uncertainty: the influence of Bayesian statistics and cognitive psychology, *Conservation Ecology* vol 2, no 1.
- [9] Anderson R, Moore T 2008, Information Security Economics and Beyond, Information Security Summit 2008.
- [10] 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.
- [11] 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.
- [12] Axelrod R 1984 *The Evolution of Cooperation* Harmondsworth UK, Penguin.
- [13] 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.
- [14] Baddeley M 2006, Behind the Black Box: a survey of realworld investment appraisal approaches *Empirica*, vol 33, no 5, pp 329-350.
- [15] 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.
- [16] 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.
- [17] Banerjee A 1992, A Simple Model of Herd Behavior, *Quarterly Journal of Economics*, vol 107, no 3, pp 797-817.
- [18] 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.

- [19] 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.
- [20] Basili M and Zappia C 2009, Shackle And Modern Decision Theory, *Metroeconomica*, vol 60, no 2, pp 245-282.
- [21] 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.
- [22] Blackmore S 1999, *The Meme Machine*, Oxford, Oxford University Press.
- [23] 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.
- [24] Bonneau J and Preibusch S 2009, The Privacy Jungle: On the market for Data Protection in Social Networks, WEIS 2009.
- [25] Brunnermeier M 2001, *Asset pricing under asymmetric information*, Oxford, Oxford University Press.
- [26] Bulmer M G 1979, *Principles of Statistics*, New York, Dover.
- [27] Clark 2010, A social embedding of network security: trust, constraint, power and control, *Security and Human Behaviour* 2010.
- [28] Davidson P 1991, Is Probability Theory Relevant for Uncertainty? A Post Keynesian Perspective, *Journal of Economic Perspectives*, vol 5, pp 129-143.
- [29] Dawkins R 1976, *The Selfish Gene*, Oxford, Oxford University Press.
- [30] DellaVigna S and Malmendier U 2006, Paying Not to Go to the Gym *American Economic Review* vol 96, no 3, pp 694-719.
- [31] Economides N 1996, The Economics of Networks, *International Journal of industrial Organisation* vol 14, no 6, pp 673-99.
- [32] Eichenberger 2001, Economic incentives transform psychological anomalies, in Felto- vich F J, Ford K M and Hoffman R R *Expertise in Context: Human and Machine*, Cambridge MA: MIT Press, pp 21-36.
- [33] Elster J 1996, Rationality and the emotions, *Economic Journal*, vol 106, no 438, pp 136-197.
- [34] Elster J 1998, Emotions and economic theory, *Journal of Economic Literature*, vol 36, no 1, pp 47-74.
- [35] 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.
- [36] Laibson, D 1997, Golden eggs and hyperbolic discounting, *Quarterly Journal of Economics* vol 112, pp 443-477.

- [37] Gigereznar G 2007, *Gut Feelings*, London, Allen Lane.
- [38] Gigereznar G and Goldstein DG 1996, Reasoning in a fast and frugal way: models of bounded rationality, *Psychological Review*, vol 103, pp 650-669.
- [39] Hirshleifer J 1983, From weakest link to best shot: the voluntary provision of public goods, *Public Choice*, vol 41, no 3, pp 371-386.
- [40] Gould P 1970, Is *Statistix inferens* the geological name for wild goose. *Economic Geography* vol 46, pp 438-448.
- [41] Kahneman D and Tversky A 1973, On the psychology of prediction, *Psychological Review*, vol 80, pp 237-51.
- [42] Kahneman D and Tversky A 1979, Prospect Theory: An Analysis of Decision under Risk, *Econometrica*, vol 47, no 2, pp 263-292.
- [43] Katz M L and Shapiro C (1994) Systems Competition and Network Effects, *Journal of Economic Perspectives*, vol 8, no 2, pp 93-115.
- [44] Kennedy P 1998, *Guide to Econometrics*, Oxford, Blackwell.
- [45] Keynes J M 1921, *A Treatise on Probability*, Macmillan, London.
- [46] Keynes J M 1930, *Treatise on Money*, Macmillan, London.
- [47] Keynes J M 1936, *The General Theory of Employment, Interest and Money*, Macmillan, London.
- [48] Keynes J M 1937, The General Theory Of Employment, *Quarterly Journal of Economics*, vol 51, pp 209-223.
- [49] 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.
- [50] 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.
- [51] 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.
- [52] Lynch A 1996, *Thought Contagion: How Belief Spreads Through Society*, New York, Basic Books.
- [53] Lynch A 2003, An introduction to the evolutionary epidemiology of ideas, *The Biological Physicist*, vol 3, pp 7-14.
- [54] Minsky 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.

- [55] Odlyzko A 2003, Economics, Psychology, and the Sociology of Security, *Financial Cryptography 2003*.
- [56] O'Donoghue T and Rabin M 1999, Doing It Now or Later, *American Economic Review*, vol 89, no 1, pp 103-24.
- [57] O'Donoghue T and Rabin M 2001, Choice and Procrastination, *Quarterly Journal of Economics*, vol 116, no 1, pp 121-160.
- [58] 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.
- [59] Shackle G L S 1953, The logic of surprise, *Economica*, vol 20, pp 112-117.
- [60] Shapiro C and Varian H R 1998, *Information Rules: A Strategic Guide to the Network Economy* Massachusetts, Harvard Business School Press.
- [61] Scharfstein D S and Stein J C 1990, Herd behaviour and investment, *American Economic Review*, vol 80, no 3, pp 465-79.
- [62] Schultz W 2006, Behavioral theories and the neurophysiology of reward, *Annual Review of Psychology*, vol 57, pp 87-115.
- [63] Shiller R J 1995, Conversation, Information and Herd Behavior, *American Economic Review*, vol 85, no 2, pp 181-85.
- [64] Shiller R J 2000, *Irrational exuberance*, Princeton, Princeton University Press.
- [65] Shiller R J 2003, From Efficient Markets Theory to Behavioral Finance, *Journal of Economic Perspectives*, vol 17, no 1, pp 83-104.
- [66] 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.
- [67] Schwarz N 2000, Emotion, cognition and decisionmaking, *Cognition and Emotion*, vol 14, pp 433-440.
- [68] Shy O 2001, *The Economics of Network Industries*, Cambridge, Cambridge University Press.
- [69] Simon H 1979, From substantive to procedural rationality, in F H Hahn and M Hollis (eds), *Philosophy and Economic Theory*, Oxford, Oxford University Press.
- [70] Skinner D C 1999, *Introduction to Decision Analysis*, Delaware, Probabilistic Publishing.
- [71] Sornette D 2003, *Why Stock Markets Crash: Critical Events in Complex Financial Systems*, Princeton, Princeton University Press.
- [72] Thaler R H and Sunstein C 1999, Mental Accounting Matters, *Journal of Behavioral Decision Making*, vol 12, no 3, pp 183-206.

- [73] Thaler R and Sunstein C 2008, *Nudge: Improving Decisions about Health, Wealth and Happiness* Yale: Yale University Press.
- [74] Topol R 1991, Bubbles and volatility of stock prices: effect of mimetic contagion, *Economic Journal*, vol 101, no 407, pp 786-800.
- [75] Tversky A and Kahneman D 1974, Judgement under uncertainty: heuristics and biases, *Science*, vol 185, 1124-1131.
- [76] 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.
- [77] Varian H 2004, *Intermediate Microeconomics*, Norton Publishing.