script*ed*

Volume 4, Issue 4, September 2007

Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective

Anne Savirimuthu and Joseph Savirimuthu***

Abstract

The Fraud Act 2006 provides us with an instrument through which we can now target emerging online criminal threats posed by identity thieves. This paper argues for a nuanced approach to the debates regarding the amenability of online criminal activity to centralised regulatory oversight. Managing risks in a decentralised and distributed network environment has frequently descended into a question of how liability rules can be harnessed to promote trust and security. We argue that a deeper understanding of the governance implications of managing complex systems is an important prerequisite to coherent policymaking. The analysis advocated in the paper has a number of implications for the way we understand and conceptualise information security governance in the online environment. We identify three. First, law is a necessary but not a sufficient governance instrument in managing the emerging threats on the Internet. Second, identity theft is a social not technologically driven problem. Third, emerging networks for information sharing, the evolution of specialised technological solutions and increased end-user participation suggest an important trend in the way online threats can be conceptualised and managed. The

* Senior Lecturer in Law - University of Central Lancashire: aesavirimuthu@uclan.ac.uk

**Lecturer in Law - Liverpool Law School, University of Liverpool: jsaviri@liverpool.ac.uk
Joseph is also a Consultant(Academia) with The Mediation Room:
jsavirimuthu@themediationroom.com

central thesis of the paper is that Luhmann's ideas of autopoiesis and social systems may provide us with a better understanding of governance in the online environment than what seems to be afforded by current analysis of the Fraud Act 2006.

DOI: 10.2966/scrip.040407.436

1. Introduction

Identity theft, phishing and pharming have suddenly raised issues in respect of law's inability to deter perpetrators of such criminal activities. There is some justification for the growing concerns. The "Internet Security Threat Report" issued on September 17, 2007 describes the increased use of the Internet and its resources to facilitate identity theft, and the acquisition of personal and sensitive information to undertake online criminal activity. The Anti-Phishing Working Group, noted that 23917 unique phishing reports were received in July 2007.[1] The number of unique phishing sites created for this month was estimated at 30999. According to Symantec, criminals have at their disposal new and sophisticated technologies.[2] Criminals are now using websites as malware vectors. Computers of visitors to legitimate web sites can now be infected by 'drive-by' malware. Identity fraud is a growing problem. According to APACS, the UK payments association, identity theft imposes significant economic burdens.[3] Costs have been estimated to be around £504.8m. These are losses resulting from plastic cards used by persons appropriating the identity of a rightful owner or fictitious identity.[4] The Home Office Identity Fraud Steering Committee reports that identity fraud costs the UK economy £1.7 billion.[5] Can the law, and in particular, the criminal law, be used to steer through social norms which will sustain trust and confidence in the online environment? This is an important question – the Fraud Act 2006 is seen as undertaking a strategic regulatory role. However, it is submitted that the maintenance of trust and confidence in the online environment is not purely a public law matter. The borderless nature of online activities highlights the private dimension of information security governance. Is law therefore an apposite mechanism through which social policies regarding responsible computer use and prudent risk management and assessment be achieved? This paper argues for a nuanced approach to the debates regarding the amenability of online criminal activity to centralised regulatory oversight. Managing risks in a decentralised and distributed network environment has frequently descended into a question of how liability rules can be harnessed to promote trust and security. We argue however that a deeper understanding of the governance implications of managing complex systems is an important prerequisite to informed and coherent policymaking. This paper will not re-visit issues relating to the economics of cybersecurity or whether Internet Service Providers and software manufacturers should assume greater responsibility for the losses resulting from identity theft. These are of course important questions. That said, we submit that an understanding of the threat landscape in the context of complex social systems and its significance for the Fraud Act 2006 may provide us with a better grasp of the reality of governance in the Internet. Accordingly, the analysis advocated in the paper has a number of implications for the way we currently view the role of the Fraud Act 2006 in relation to identity theft. We identify three.

[1] http://www.antiphishing.org/reports/apwg_report_july_2007.pdf.

[2] http://www.symantec.com/business/theme.jsp?themeid=threatreport.

[3] http://www.apacs.org.uk/media_centre/press/05_03_08.html.

[4] http://www.identity-theft.org.uk/ID%20fraud%20table.pdf.

[5] http://www.identity-theft.org.uk/what-is-being-done.htm.

First, law is a necessary but not a sufficient governance instrument in managing emerging threats on the Internet. Second, identity theft is a social not technologically driven problem. Third, emerging networks for information sharing, the evolution of specialised technological solutions and increased end-user participation suggest an important trend in the way online threats can be conceptualised and managed. The central thesis of the paper is that Luhmann's ideas of autopoiesis and social systems may provide us with a better understanding of governance in the online environment than what seems to be afforded by current analysis of the 2006 Act.

2. Law and "Right Answers"

It is uncontroversial that the criminal law is an important instrument of social policy.[6] The State's monopoly over the coercive machinery of the criminal law corresponds very much with the importance individuals attach to order and security. The criminal law can also be viewed as a significant instrument for promoting compliance with accepted standards of behaviour and norms.[7] It also has symbolic value. The rules and norms of behaviour commonly correspond with society's normative expectations of what constitutes acceptable conduct. It is therefore not surprising that when criminal activities migrate into the online environment, we see various strands of the normative role of the criminal law weaving themselves into the debates on governance. The criminal law is now seen as having an important role in finding the 'right answers' to the evolving threats posed by identity thieves.

'Identity theft' is defined by the Oxford English dictionary as comprising the dishonest acquisition of personal information in order to perpetrate fraud, typically by obtaining credit, loans, etc., in someone else's name.[8] Chawki and Wahab have rightly noted that the term identity is often used in an arbitrary and imprecise manner in popular media and literature.[9] It is arguable that the appropriation of an identity of itself will not give rise to a criminal offence.[10] These matters are not the concern of the paper in the light of the Fraud Act 2006. We can now illustrate how law views the activity of phishing.[11] Phishing is an online activity that uses social engineering strategies and technical ploys to gain access to an individuals' personal identity, data and other information.[12] Phishing attacks harness the technology of the Internet and

[6] A M Polinsky and S Shavell, "The Economic Theory of Public Enforcement of Law", (2000) 38 *Journal of Economic Literature*, 45-77.

[7] G Becker, "Crime and Punishment: An Economic Approach", (1968) 76 (2) *Journal of Political Economy*, 169-217.

[8] http://dictionary.oed.com.

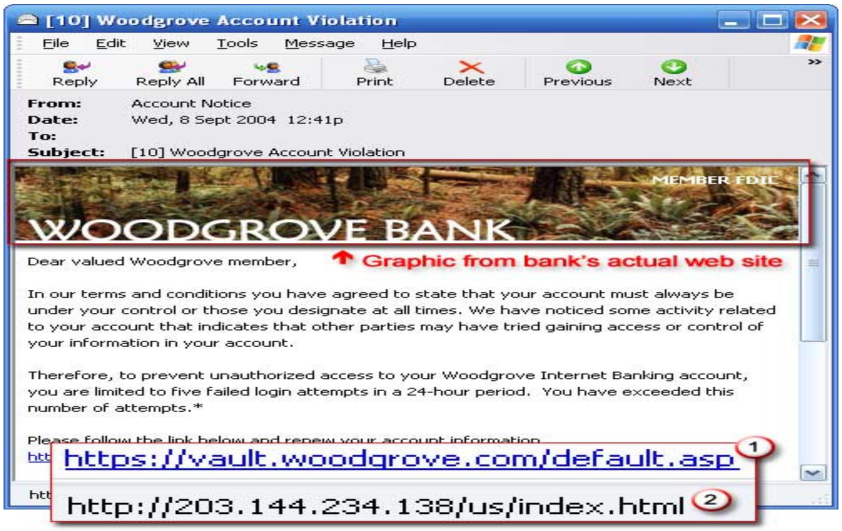
[9] M Chawki and M Wahab, "Identity Theft in Cyberspace: Issues and Solutions", (2006) 11 (1) *Lex Electronica* http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.htm.

[10] See Memorandum from the Society for Computers and Law—Internet Interest Group and Privacy and Data Protection Interest Group paragraph 5. http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/7012402.htm and Home Office Identity Fraud Steering Committee: http://www.identity-theft.org.uk/definition.htm.

[11] We draw on the accounts provided by the Symantec Threat Report http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf.

[12] http://www.antiphishing.org/.

software to create fraudulent emails. In the example below, a victim receives a phishing email purporting to come from a trusted party, Woodgrove Bank. This email has a link to a fraudulent website. The email and the creation of a fraudulent website are designed to trick the unsuspecting individual to think that Woodgrove Bank has been the initiator of the communication. Spoof emails and websites like this are frequently used by phishers to gain unauthorised access to a range of information, which includes personal data, usernames and passwords and financial information.



From: Account Notice
Date: Wed, 8 Sept 2004 12:41p
To:
Subject: [10] Woodgrove Account Violation

Dear valued Woodgrove member,

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

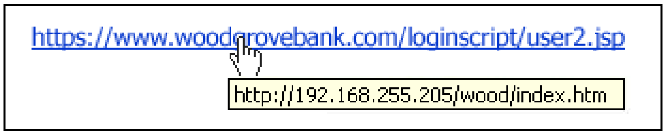
Please follow the link below and renew your account information

https://vault.woodgrove.com/default.asp

http://203.144.234.138/us/index.html

(source: www.microsoft.com)

As these two examples show, the victim is led to trust the authenticity of the source since the fraudulent link appears to have the same URL as the trusted source. The link here can be said to be “masked”. The real website is the hidden url:[13]



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

What is particularly significant about the Fraud Act 2006 is that the act of sending such emails will in itself give rise to prosecution. There is no requirement for the phisher to be shown to have used the information to access the funds in the victim’s account. The victim need not respond to the email or act on the request. The 2006 Act, which was enacted to keep abreast of emerging technologies and to obviate the need for constant reactive reform, appears to facilitate the prosecution of phishing,

[13] http://www.microsoft.com/protect/yourself/phishing/identify.mspx.

demanding neither proof of deception nor the obtaining of any property, which were pre-requisites to conviction under the previous legislation.[14] Section 1 of the 2006 Act creates a new general offence of 'fraud', which can be committed in three ways: by false representation (s2); by failing to disclose information (s3); and by abuse of position (s4). Section 2, with which we are primarily concerned here, provides as follows:

'(1) A person is in breach of this section if he—

(a) dishonestly makes a false representation, and

(b) intends, by making the representation—

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.'

Section 2 sub-sections (2) and (3) respectively, state that representation means any representation as to fact or law and that a representation may be expressed or implied. In other words, there is no limitation on the way a representation must be made and it will therefore include a representation being in written or spoken form, or where it is posted on a website or email. The 2006 Act will cover all forms of phishing activity. These include, sending of spoof emails to unsuspecting businesses and individuals ('vishing') and spear phishing. In spear phishing, the email looks very much like an authentic email one expects to receive from an employer, business or organisation.[15] In this phishing attack, the recipient may submit relevant information like passwords and login information as they assume that the request has come from a trusted person within that organisation or business. Thus in the context of phishing activity, the *actus reus* of the section 2 offence is fulfilled when the initial email requesting the recipient to access a given website is received and read. The email constitutes an implied representation that it is from a legitimate source. With respect to *mens rea* requirements for section 2, the first element that must be proved by the prosecution is that the phisher made the representation dishonestly, which is not defined by the 2006 Act, and which remains a question of fact for the jury.[16]

The second element to be proved is that the phisher must know that his representation is or might be untrue or misleading (s2(2)(b)). Third, the phisher must intend, by the false representation to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss. Section 5 provides that both these elements extend only to gain or loss in money or other property; and include any such gain or loss whether temporary or permanent. Property here is understood to cover any property whether real or personal (including things in action and other intangible property). "Gain" includes a gain by keeping what one has, as well as a gain by getting what one does not have. "Loss" includes a loss by not getting what one might get, as well as a loss by parting with what one has. The broad definition in section 2 is also technologically neutral. This is particularly significant since law can now accommodate new forms of subterfuge.

[14] Sections 15 and 15A Theft Act 1968.

[15] See http://www.microsoft.com/protect/yourself/phishing/spear.mspx.

[16] See *R v Ghosh* [1982] QB 1053.

Although the criminal law continues to fulfil an important role in coordinating the way individuals organize their behaviour, its ability to deter identity theft and more generally cybercrimes has come under increased scrutiny.[17] Some have questioned whether the orthodox assumptions made about the regulatory capabilities of the criminal law necessarily bear true in the online environment.[18] Others have located the sub-optimal capabilities of the criminal law on a range of variables - resources, perceptions about the low detection and prosecution rates, the relatively low costs and ease with which cybercrimes can be perpetrated, and the gains to be made by using low cost high return strategies.[19] For example there is increasing evidence that many of the vulnerability exploits are the result of an active grey market in phishing and cybercrime toolkits.[20] The Sumitomo Bank in London was the subject of such an attack. Thieves installed a keylogger into the bank's computer. A keylogger can be purchased at the cost of £35. This device can be used to record the strokes made on a computer keyboard.[21] A phisher can obtain up to 2 million keystrokes from a keylogger. In the case involving Sumitomo Bank, the thieves were attempting to transfer £220 million out of the bank's account.[22] Another example of the ease with which cybercrimes can be committed is in the recent successful attempt by a group of online thieves in assuming the identity of ten account holders and transferring large sums of money out of the banks.[23] These incidents not only illustrate the ease with which security can be compromised but they remind us that the management of risk is not purely a public goods problem. More importantly, the ability of the criminal law as an instrument for steering through social policies must now contend with the scale of the governance challenges that the online environment now poses. Organisational information security oversight and poor safe computing practices by individuals contribute to the rise of identity theft. Law, it is submitted, is a necessary but not sufficient mechanism through which identity theft can be tackled. One way through which we can expand the narrative of governance is with this query: assume that absolute online security is not possible and that you are charged with the responsibility of devising solutions to promote trust and security. What would be your commencing point? Wall's commencing point is that we can encode legal norms and values – code is law.[24] He does not dwell on this since he acknowledges that measuring the effectiveness of legal regulation poses insuperable difficulties.[25]

[17] L B Benson, K Iljoong and D W Rasmussen, "Estimating Deterrence Effects: A Public Choice Perspective on the Economics of Crime Literature", (1994) 61 *Southern Economic Journal*.

[18] S Cameron, "The Economics of Crime Deterrence: A Survey of Theory and Evidence", (1988) 41 (2) *Kyklos*, 301-323.

[19] N Kshetri, "The Simple Economics of Cybercrimes", *IEEE Security & Privacy*, January/February 2006, 33-39.

[20] CBS News, "Hackers getting more professional", September 17, 2007 Available at http://www.cbsnews.com/stories/2007/09/17/tech/main3267347.shtml?source=search_story.

[21] http://www.kmint21.com/keylogger/.

[22] See J Leyden "Cyber cops foil £220 million Sumitomo bank raid", 17 March 2005 http://www.channelregister.co.uk/2005/03/17/sumitomo_cyber-heist_foiled/.

[23] http://www.timesonline.co.uk/tol/news/uk/crime/article2759818.ece.

[24] D Wall, *Cybercrimes: The Transformation of Crime in the Information Age* (Polity Press, 2007) 187-189.

[25] Ibid. 188.

Software can be used as part of the standard setting and regulatory agenda. The issue of benchmarking is important – but it is not a problem that is unique to online crimes. Additionally, design solutions in the form of anti-identity theft software, can be counterproductive if we ignore "human" systems. Too often breaches in security can be linked to end users becoming complacent or careless with passwords and usernames. Others have focused, for example, on the way legal liability rules, could be harnessed to distribute existing burdens borne by society generally, the available options for imbuing social norms and standards into software and the strategies for securing compliance.[26] Consistent with this line of policy deliberation is Anderson's call for a re-assessment of the existing liability rules and that software vendors should now be made to shoulder greater responsibility.[27] Legal rules can be used to influence the way individuals approach risks.[28] This point is underscored by the recognition that many software manufacturers and businesses do not attach sufficient importance to information security:[29]

> *"We see 'take-down' as a reactive strategy, an increasingly prevalent trend in the way that security issues are being handled. Software vendors wait for vulnerabilities to be discovered and then issue patches. Anti-virus tools update their databases with new signatures as new viruses are identified. In these reactive approaches, the defenders aim to identify the bad guys as quickly as possible to minimise exposure, while the bad guys scramble to open new holes at a sufficiently fast rate to continue their activities."*

There is however a more problematic aspect to information security governance – this is to do with the problem of managing complex social systems. Many have observed that the Internet is a complex network of networks.[30] Murray, for example, has no doubts that in the Internet:[31]

> *"…the process of regulation is...complex. All parties in a regulatory environment continually and simultaneously act as regulator and regulatee. Changes within the regulatory environment are therefore constant and as a result the first stage in designing a regulatory*

[26] See generally Select Committee on Science and Technology, *5th Report on Personal Internet Security* (London: The Stationery Office Limited, 2007) (hereinafter *5th Report on Personal Internet Security*).

[27] R Anderson, "Why information security is hard: An economic perspective", (2001). Presented at the 18th Symposium on Operating Systems Principles, October 21-24, Lake Louise, Alberta, Canada; also the 17th Annual Computer Security Applications Conference, December 10-14, New Orleans, Louisiana; http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf.

[28] L Gordon and M Loeb, "The economics of information security investment", ACM Transactions on Information and System Security (2002) 5 (4), 438-457, S Skaperdas, "Conflict and attitudes toward risk", (1991) 81 *American Economic Review*, 116-120.

[29] T Moore and R Clayton, "An Empirical Analysis of the Current State of Phishing Attack and Defence", http://weis2007.econinfosec.org/papers/51.pdf. Workshop on the Economics of Information Security, 2007.

[30] A Murray, *The Regulation of Cyberspace* (UK: GlassHouse, 2007) 250-251.

[31] Ibid. 250.

> *intervention in any complex regulatory environment, including cyberspace, is to develop a dynamic model of the environment, recording all parties and mapping their contemporary regulatory settlements with each other. Second, by observing this environment, regulators are required to map the communications dynamic in place within this regulatory matrix…all that is required is that the dynamic of such communication is mapped. In other words, the regulator need not anticipate the needs of all actors in the regulatory matrix; they need only anticipate the regulatory tensions that are likely to arise when actors communicate. Finally, once a regulatory intervention has been designed, it should be tested thoroughly."*

What does that entail in policy and strategic terms in the specific context of identity theft and phishing? In setting out an organic regulatory framework, Murray is drawing on some of the insights generated by systems theorists, in particular Niklas Luhmann. There is much to commend his analysis. In attempting to emphasise the complexity of the governance process however, Murray fails to highlight one of the fundamental insights offered by Niklas Luhmann – sub-systems such as markets, law and politics have structures and processes that are self-referential and preserve their own distinctiveness.[32] This is a critical insight for two reasons. First, juridicalisation is only one means through which complex social problems and risks are defined.[33] Second, if we accept that society is a complex system, it is imperative that we have a plausible explanation as to why its order is possible in an environment of autonomous self-preserving social systems.

Before we can begin the task of unpacking the insights of Luhmann, we need to approach the problems posed by identity theft differently. Let us for example begin by reformulating the central tenets of Murray's propositions in the following manner: what makes private ordering in the online environment complex? Two features of the online environment, it is suggested, challenge the orthodox approach in attempting to coerce individuals to internalize acceptable norms of behaviour: first, the technical infrastructure enables asynchronous interactions in decentralised and distributed networks; and second, the presumptive norm of access contributes to the ease with which identity thieves and phishers mobilise resources of the Internet to externalise onto society the costs of any actions.[34] As Walden noted in his testimony before the Select Committee on Personal Internet Security:[35]

> *"It is all data. It is all zeros and ones, which go across the network, whether it is a virus, a child abuse image or a political statement. Our ability to distinguish at a network level the stream of data*

[32] Ibid. 244-248.

[33] M King, "What's the Use of Luhmann's Theory?" in M King and C Thornhill (eds), *Luhmann On Law and Politics* (Oxford: Hart, 2006) 46-47. See later discussion on the significance of autopoietic social systems for information security governance.

[34] See generally the panel papers organised by the Yale Information Society Project, The Global Flow of Information (2004) available at http://islandia.law.yale.edu/isp/GlobalFlow/index.html.

[35] *5th Report on Personal Internet Security*, *supra*, n 26 at Q390.

> *which is passing is difficult without perhaps capturing too much legitimate data or not capturing the illegitimate data."*

It is of course true that we are dealing with data – notwithstanding the medium, we are still faced with a long-standing societal problem of deviants in society threatening value. Like Murray, the extract above does not assist us in any meaningful way other than to remind us that the end-to-end architecture embeds the norm of legitimacy in all communications. Instead of focussing on data or the organic regulatory model, let us remind ourselves of the scale of the threat landscape. CIFAS, the United Kingdom's Fraud Prevention Service has remarked on the rise in cases of most types of financial fraud during the first half of 2007, when compared with the same period in 2006.[36] During the first six months of 2006, Symantec reported an 86 per cent increase in phishing messages per day.[37] The large numbers of phishing activities were directed at the financial services and banking sectors. For example, the banking industry estimated that phishing frauds cost the industry £22 million in the first half of 2006.[38] A British man was recently sentenced for four years for operating an eBay Internet auction scam. He accessed account details from users and assumed their online identities to perpetrate these scams.[39] The Select Committee has commented on the ease with which criminals are now imposing negative externalities on society generally.[40] These examples illustrate the scale and reach of the evolving threats posed by identity thieves. More importantly, for present purposes, rather than focus on 'data' or the constitutional aspects of content filtering, we could direct our efforts instead on how sub-systems in society view risk and assess their relevance for information security governance.

Let us begin with a seemingly uncontroversial observation about the risk society. Society, according to Beck, responds to increased risks reflexively. For example, concerns about the threats posed by evolving risks from identity thieves, denial of services attacks, malware and viruses, result in risk being problematised by society. The characterization of particular risks as a 'problem' is treated as an important prerequisite to communications becoming part of the public discourse.[41] The juridical model of risk management is one part of this reflexive landscape. Reflexive modernisation is a form of self-confrontation. Beck regards this process as a form of societal critique of itself. It involves:[42]

[36] See http://www.cifas.org.uk/default.asp?edit_id=715-57.

[37] http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf. In the last half of 2005 over 86,906 phishing messages were detected, whilst in the first half of 2006, the numbers increased to 157,477.

[38] See BBC News, "Which? highlights Phishing losses", 28 February, 2007 http://news.bbc.co.uk/1/hi/business/6401079.stm.

[39] See BBC News, "Identity Theft Fraudster, guilty" 30 November, 2006

http://news.bbc.co.uk/1/hi/england/london/6196802.stm.

[40] *Supra*, note 26.

[41] U Beck, Risk Society: Towards a New Modernity (London: Sage, 1992) 21.

[42] U Beck, "Risk society and the provident state" in S Lash, B Szerszinski and B Wynne (eds), *Risk, Environment and Modernity: Towards a New Ecology* (London: Sage, 1996) 27-43, 34.

> *"the combination of reflex and reflections which, as long as the catastrophe itself fails to materialise, can set industrial modernity on the path to self-criticism and self-transformation. Reflexive modernisation contains both elements: the reflex-like threat to industrial society's own foundations through a successful further modernisation which is blind to dangers, and the growth of awareness, the reflection on this situation."*

The reflexivity process is not entirely dissimilar from the governance model proposed by Murray. Beck's understanding of the process of risk management involves a two-step phase. First, the risks created by new technologies must be identified. Second, the "self-confrontation" phase occurs when individuals, policymakers and society undertake a debate about how the risks are to be managed. Reflexive modernisation, in short can be likened to a political, legal, and cultural form of creative destruction.[43] Beck's reflexive thesis however, gives little weight to the way autonomous sub-systems conceptualise risk or that social systems do not operate under a universal goal. [44] This is a conclusion that can be drawn when reflecting on Murray's exposition. Murray's regulatory model can however be viewed as taking us in the right direction, but only to the extent that it draws our attention to the limits of law as an instrument of standard setting and private ordering. The question, how do social systems such as law, markets, or politics, for example, make sense of risk needs an answer if we seek a coherent and balanced understanding of the emerging information security governance challenges. Highlighting the need for responsive and nuanced regulation is important. Drawing attention to the deficiencies of the law is a necessary part of this enterprise. In both instances however, the insights generated do not assist us in grasping the particular way sub-systems such as law function in the social system. As King and Thornhill observe:[45]

> *"Any sociological examination of risks as a product of decision, therefore, should be conducted by observing the various ways in which these make sense of future uncertainty and attribute their control and management to decision-making. For Luhmannian sociology, the problematic of risk becomes, therefore, not simply how each functional subsystem is to deal effectively with risks, but how each system conceptualises risk in* its own terms *and is able (or unable) to contribute to a general societal belief that risks are indeed controllable, and avoidable through a process of causal attribution."*

The question therefore is not how sub-systems such as law, economy, or politics deal or ought to deal with risks. According to Luhmann, the autopoietic processes of

[43] U Beck, "The reinvention of politics: towards a theory of reflexive modernization", in U Beck, A Giddens, and S Lash, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Cambridge: Polity Press, 1994) 1-55, 2.

[44] See GAO Report, "Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses", available at http://www.gao.gov/new.items/d07837.pdf (accessed, 17 August, 2007).

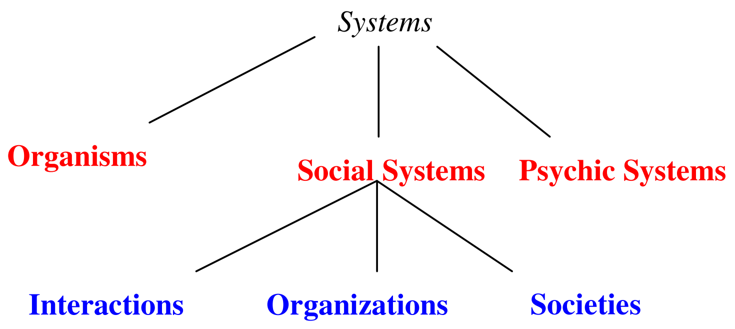
[45] M King and C Thornhill, *Niklas Luhmann's Theory of Politics and Law* (Basingstoke: Palgrave Macmillan, 2005) pp 183-184.

functionally differentiated sub-systems and their significance for the way events are reconstructed merit *a priori* analysis.

3. Autopoiesis and Social Systems: Niklas Luhmann

3.1 Niklas Luhmann and *Law as a Social System*

Systems theory has been used by many disciplines to understand and analyse complex phenomena and situations.[46] This theory departs from the anthropocentric emphasis that typifies the way we approach a wide range of legal topics. Systems' thinking on the other hand requires us to view events, situations in society, and decision making structures in organisations and intra-organisations as being constituted by complex and interdependent processes.[47] According to Luhmann, society can be understood in terms of autonomous spheres of sub-systems, which undertake different social functions.[48] Luhmann's view of sub-systems can be depicted in the following manner:



As he observes:[49]

> *"…systems make and continue to make a difference between the system and its environment. Every single operation that contributes to the self-reproduction of the system- that is, in the case of society, every single communication - reproduces this difference. In this sense, societies are operationally closed systems. They cannot*

[46] N Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press,1961) (Orig Pub 1948) p162, H Maturana and F Varela, *Autopoiesis and cognition* (D Reidel: Dordrecht, Holland, 1972) pp xi-xvii.

[47] L von Bertalanffy, *General Systems Theory. Foundations, Development, Applications* (London: Allen Lane, 1968) and WR Ashby, *An Introduction to Cybernetics* (London: Chapman and Hall Ltd, 1956).

[48] J Priban and D Nelken, "Introduction" in J Priban and D Nelken (eds) *Law's New Boundaries* (England: Ashgate Dartmouth, 2001) 1.

[49] N Luhmann, "Why Does Society Describe itself as Postmodern" in W Rasch (ed), *Observing Complexity: Systems Theory and Postmodernity* (US: Univ of Minnesota Press, 2000) 36.

> *operate outside their own boundaries. Nevertheless, the system can use its own operations to distinguish itself from its environment. It can communicate about itself (about communication) and/ or about its environment. It can distinguish between self-reference and hetero-reference, but this has to be done by an internal operation."*

Luhmann's preference for using social systems as an explanatory framework in understanding phenomena can be gleaned from his observation that modern society has evolved from segmented and stratified hierarchies to spheres of functionally differentiated social systems.[50] This paradigm shift requires us to reassess the way we conceptualise society and its regulatory institutions. According to Luhmann, networks of communications constitute society.[51] All communications take place in society.[52] The basic components of communication include interactions and communications within society. The elementary units of meaningful communications are constituted by the synthesis of information, communication and comprehension. [53] As Mingers notes:[54]

> *"information is what the message is about, utterance is the form in which it is produced together with the intentions of its sender, and understanding is the meaning that it generates (which can include misunderstanding) in the receiver."*

Luhmann's constructivist epistemology in respect of the way meaning in communications is reconstructed deploys a second order observation of society (i.e. communications involve observations about communications).[55] Communications, and not individuals become the objects of observation. Luhmann is particularly interested in understanding how sub-systems such as politics, markets and law reconstruct discrete meanings from one single event. For example, a phishing attack would be viewed by law as an 'illegal act'. A purchase of an anti-phishing kit by a consumer or an organisation would be viewed by the economy as a market transaction. Communications arising from identity theft will be reconstructed by sub-

[50] Ibid. 42.

[51] J Mingers, "Can social systems be autopoietic? Assessing Luhmann's social theory" (2002) 50 (2) *The Sociological Review*, 278–299. See also J Mingers, "Can Social Systems be Autopoietic? Bhaskar's and Giddens' Social Theories" (2004) 34 (4) *Journal for the Theory of Social Behaviour*, 403–427. Cf. M King and C Thornhill, "'Will the real Niklas Luhmann stand up, please'. A reply to John Mingers" (2003) 51 (2) *The Sociological Review*, 276–285.

[52] The following accounts draw on H-G Moeller, *Luhmann Explained: From Souls to Systems* (Chicago and La Salle, Illinois: Open Court, 2006) and M King and C Thornhill, *Niklas Luhmann's Theory of Politics and Law* (Basingstoke: Palgrave Macmillan, 2005).

[53] M King and A Schutz, "The Ambitious Modesty of Niklas Luhmann" (1994) 21 *Journal of Law and Society* 261.

[54] J Mingers, "Can social systems be autopoietic? Assessing Luhmann's social theory" (2002) 50 (2) *The Sociological Review*, 278–299.

[55] This section provides a synthesis of Luhmann's ideas. According to Luhmann social systems communicate by talking about talking or writing about writing: N Luhmann, *Observations on Modernity*. (Translated W Whobrey) (Stanford University Press: Stanford, CA, USA, 1992) and N Luhmann, *Social Systems*, (Translated J Bednarz Jr, D Baecker) (Stanford University Press: Stanford, CA, USA, 1995).

systems according to their structures and processes: law (for example, in the form of the legal and evidentiary rules under the Fraud Act 2006), economy (the collation of banks financial statistics), education (in the form of Internet Service providers and the Anti-Phishing Working Group's assessment of the impact of these criminal activities on trust and confidence) and politics (reflecting public concerns and responding to the need for legislation).[56] Luhmann's emphasis on the meaning construction role of sub-systems needs to be considered along with the inferences he draws from his proposition that society is also an autopoietic system.[57] Society is autopoietic in the sense that it has structures and processes that enable it to produce and reproduce itself.[58] Law, according to Luhmann is one example of an autopoietic sub-system.[59] Sub-systems may evolve and reflect the complex realities of the environment. For example, in highly integrated and technologically advanced societies sub-systems such as politics, law, economy and education mirror the complexities of the environment in its structures and processes. Agrarian or less advanced societies will have sub-systems that are less complex and structures that model the relative simplicity of its environment.[60]

One should be careful however in drawing generalised conclusions from the comparison between social and biological autopoiesis.[61] In scientific terms there is a wide gap between the autopoiesis of cells, organs and the nervous systems and that of the process by which society evolves, adapts and reproduces.[62] Luhmann's use of second-order observation and autopoiesis should be viewed as attempt to encourage us to integrate ideas from systems into the operation of sub-systems such as law and in particular their meaning construction operations. Three observations could be offered here. First, rather than view social problems like phishing through the juridical or political framework, Luhmann highlights the significance of the relationship between the self-referential properties of sub-systems in society and the constraints systems operate under. [63] The self-referential properties are for example, necessary for systems to retain their unity and distinctiveness. Accordingly, we can think of each sub-system as possessing structures and processes that distinguish one system from the other.

[56] I modify the example provided in M King and C Thornhill, *Niklas Luhmann's Theory of Politics and Law* (Hampshire: Palgrave Macmillan, 2005) 8.

[57] M King and C Thornhill, "Will the real Niklas Luhmann stand up, please. A reply to John Mingers" (2003) 51 (2) *The Sociological Review*, 276–285.

[58] N Luhmann, "Why Does Society Describe itself as Postmodern" in W Rasch (ed), *supra*, note 49, 38.

[59] N Luhmann, *Law as a Social System* (Oxford: OUP, 2004) pp 64-66. See also G Teubner, *Law as an Autopoietic System* (Oxford: Blackwell, 1993) 9-10.

[60] N Luhmann, "Closure and Openness: On Reality in the World of Law" in G Teubner (ed), *Autopoietic Law: A New Approach to Law and Society* (Berlin: Walter de Gruyer,1988)12-36.

[61] *Supra* note 57.

[62] M King, "The Truth about Autopoiesis" (1993) 20 *Journal of Law and Society* 218.

[63] J Arnoldi, "Niklas Luhmann: An Introduction", *Theory Culture Society* (2001) 18: 1.

System	**Function**	**Efficacy**	**Code**	**Program**	**Medium**
Law	Manage Norm Expectations	Regulation of Conflicts	Legal / Illegal	Laws, regulation, constitution	Jurisdiction
Politics	Make Collective Decisions Possible	Practical Application	Government / Opposition	Goals of Political Parties/Ideologies	Power
Science	Production of Knowledge	Supply of Knowledge	True / False	Theories, methods	Truth
Economy	Reduction of Scarcity	Satisfaction of needs	Payment / Non-payment	Budgets	Money

(source: H-Georg Muller, 29)

Second, as the diagram makes explicit, social systems have functional-problem solving structures and processes. These structures and processes are self-referential. The ability of law to provide the 'right answers' is consistent with the role of its structures and meaning construction processes.[64] For example, law reconstructs the risks encountered in society as legal communications.[65] When an identity thief has been apprehended and prosecuted, law can then apply its rules to the situation. Law's unity and distinctiveness can be seen as a form of 'operational closure' - a court of law decides a conflict or prosecution on the basis of the established precedents and legal rules and not what the newspapers say should be the outcome.[66] Third, law's meaning construction processes acts as a constraint:[67]

> *"If burglars believe that their chances of getting caught are very slim, nothing that the criminal law can do will effectively control the incidence of burglary. Law, as a social communication system, simply has no way of understanding getting caught/not getting caught through its lawful/unlawful coding. All that the law may do is to encourage burglars to own up to the times when they did not get caught by making it lawful for courts to take them into account in sentencing and in doing so rule out any future prosecution. But this, of course, depends upon the burglar getting caught in the first*

[64] See for example, the emerging security flaws identified in the Apple iPhone and the information gathering processes of White Hat hackers.

[65] M Corker and J Davis, "Disabled Children: (Still) Invisible Under the Law", in J Cooper (ed), *Law, Rights and Disability* (London: Jessica Kingsley Publishers, 2000) p 219.

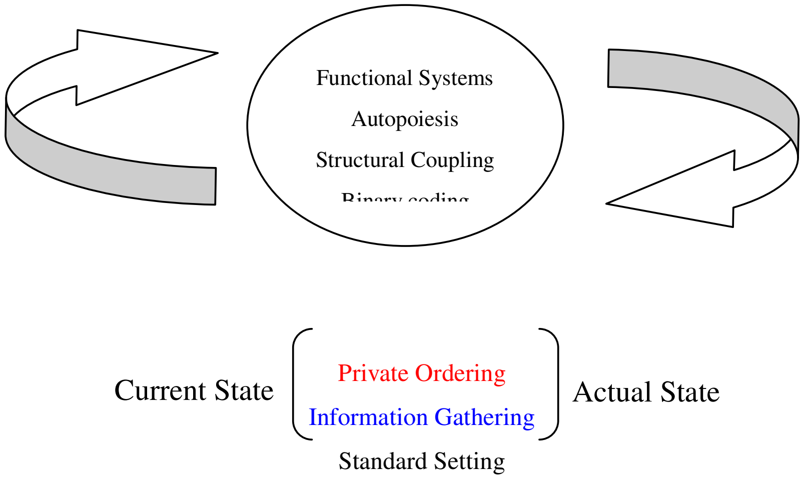
[66] N Luhmann, *Law as a Social System*, *supra*, note 48, 467.

[67] M King, "What's the Use of Luhmann's Theory?", in M King and C Thornhill(eds), *Luhmann On Law and Politics* p 46-47.

> *place. Furthermore, there may well be other factors which could reduce the number of burglaries, such as improved home security, better police detection, more police officers, neighbourhood watch etc, but these are invisible to the law, which sees only what it can see using the restricted vision of its coding."*

Functionally differentiated systems construct meaning from events in their own terms. There are limits to the ability of a system to construct meanings from events. For example, under the Theft Act 1968, law had no way of making sense of 'identity' theft. This constraint is now overcome by legislative intervention in the form of the Fraud Act 2006. It should be noted here that the emphasis shifts away from ideas of "gain" or "loss", and towards the intent of the identity thief. To be sure, following the passing of the Fraud Act 2006 the fact that machines cannot be deceived, as in the case where the phisher assumes the identity of a person to gain access to a bank account, and deceives a machine, is not considered to be an obstacle.

A related consideration is that law cannot impose its knowledge of risk onto other systems. This is a key point. Sub-systems have programmes and processes that enable them to retain their identity whilst being open to their environment. Perturbations from the environment lead to the system assessing its operations with a view to reaching its desired state.



Knowledge about risks is not static or given but is constantly being reproduced and created through interactions. Notwithstanding the constraints inherent in law, sub-systems are provided with a facility to make sense of other communications. System response to turbulence and disruption caused by information security threats is however affected by the 'time lag' between the 'actual' state and the 'desired' state. Recall that until the enactment of the Fraud Act 2006, the act of deceiving a machine could not be regarded as a form of meaningful communication. Until the enactment of the 2006 Act, law had no processes for determining the legality or illegality of 'deceiving machines'. Exchanges of information between sub-systems can however take place through the process of structural coupling. Structural coupling enables a sub-system to get to 'know' events and situations in its environment. Coding and programming enable each sub-system to make sense of its own world and process information into meaningful communications. Law's inability to deter identity thieves, for example, may lead to the perturbations being reconstructed by other sub-systems into meaningful communications. Signals to the economy can be seen in the expansion of the market for information security products and services. The market for information security is now worth $4.684 billion, which is an increase of 17.1 per cent from the previous year.[68] The economy transforms the perturbations into economic communications via the price mechanism. Law's inability to deter identity theft may lead to science producing knowledge in the form of algorithms that promote end-point security – these are coded as true/false and the input of system level software authors provide content for the various programmes. Given that identity theft deploys social engineering techniques, the education system will increase the availability of knowledge so that users can make informed decisions.

3.1 Conclusion

It should be noted that Luhmann's theory provides us with one framework for conceptualising the governance challenges facing society. This is sometimes overlooked. It may explain, for example, why it is lawyers who view the criminal law as providing 'right answers' may find Luhmann's view of autopoietic systems problematic.[69] To better understand the role of law, we need a coherent understanding of complex social systems and their implications for governance. For example, it is often assumed in discussions on the relationship between law, technology and society on the one hand and governance, risk and responsibility on the other, that software code, law or policy prescriptions from the government will be adequate to manage society which is becoming increasingly differentiated and specialised. Luhmann reminds us that ultimately sustainable systems must either model the complexity of their environment (and become more complex) or conversely reduce complexity in the environment. Communications taking place in invariant autonomous systems underscore the growing interest in seeking sustainable regulatory solutions. Luhmann's framing of society as meaningful communications and the effect of law's coding of its environment demonstrates the problematic of risk and the futility of using law to conceptualise risk in a manner that accommodates the way other autopoietic and functionally differentiated systems construct meaning of similar

[68] See Serious Organised Crime Agency, United Kingdom Threat Assessment 2006/2007, paras 2.1, 2.39 -2.40 Available at http://www.soca.gov.uk/assessPublications/downloads/threat_assess_unclass_250706.pdf.

[69] Selected bibliography: M King, "The Truth about Autopoiesis" (1993) 20 *Journal of Law and Society* 218, M King and A Schutz, "The Ambitious Modesty of Niklas Luhmann" (1994) 21 *Journal of Law and Society* 261, A James, "An Open or Shut Case? Law as Autopoietic System"| (1992) 19 *Journal of Law and Society* 271, M Neves, "From the Autopoiesis to the Allopoiesis of Law" (2001) 28 *Journal of Law and Society* 242, G Teubner, "Evolution of Autopoietic Law" in G Teubner (ed) *Autopoietic Law: A New Approach to Law and Society*, (1987a) 222, D Nelken, "Blinding Insights? The Limits of a Reflexive Sociology of Law" (1998) 25 *Journal of Law and Society* 407, at 419, G Teubner, "How the Law Thinks: Toward a Constructivist Epistemology of Law" (1989) 23 *Law and Society Review* 727, at 728, W T Murphy, "Niklas Luhmann on Law, Politics, and Social Theory" (1984) 47 *Modern Law Review* 603; A J Jacobson, "Autopoietic Law: the New Science of Niklas Luhmann" (1989) 87 *Michigan Law Review* 1647, R Lempert, "The Autonomy of Law: Two Visions Compared" in G Teubner (ed) *Autopoietic Law: A New Approach to Law and Society,* (1988) 152-190.

events.[70] Luhmann directs our focus instead towards understanding the structures and processes by which each system transforms *information in its environment* into communications *generated by the system* that serve as inputs and outputs.[71] As Leydesdorff observes:[72]

> *"The different function systems use various codes for providing meaning for communication. Whereas the hierarchical (catholic) system had only a single centre of control - that was based on a holy text - economic exchange relations, for example, could now be handled by making payments. The symbolically generalized medium of money makes it no longer necessary to communicate by negotiating prices verbally or imposing them by force. The specification of a price as an expected market value speeds up the economic transaction processes by organizing the communication in a specific (that is, functionally codified) format."*

To conclude, social systems can be viewed as bounded systems with structures and components that seek to reconcile the functions and goals of the individual system with the disturbances and conditions of the environment.[73] Communication systems can therefore be seen as engaged in a complex process of information gathering, ordering and standard setting. This is a non-linear and recursive process that involves using not only existing information but also those which are created as a result of a system's autopoietic activities. Instead of viewing governance in terms of the coordinating instruments provided by law, norms, market and technology, we can instead regard the process of self-organisation as involving complex differentiated and constructive processes by which risk is conceptualised. If we accept that communications constitute social systems, we can now assess the significance of viewing the problem of information insecurity in terms of reflexive risk communications.[74]

4. Revisiting Identity Theft

4.1 The Network of Communications

We are said to be living in the age of the information society. Our individual and collective identities are being processed and defined by electronic information networks.[75] The process of constructing the information society, the content and meaning we ascribe to it cannot be separated from the institutions, rules and norms

[70] N Luhmann, *Law as a Social System*, *supra*, note 48, pp 64-65.

[71] Ibid. p 73.

[72] L Leydesdorff, "Interaction versus action in Luhmann's sociology of communication" in C Grant (ed) *Rethinking Communicative Interaction: New Interdisciplinary Horizons* (USA: John Benjamins Publishing Company, 2003) 163, 174.

[73] C Hood, *The Government of Risk* (Oxford: OUP, 2004) pp 148-9.

[74] See also G Teubner, *Law as an Autopoietic System* (Oxford: Blackwell, 1993) Chapters 5 and 6.

[75] See for example M Castells, *The Rise of the Network Society* (Oxford: Blackwell, 2002) p7

that govern these activities.[76] New opportunities are being created for expression and the constitution of constituencies.[77] This new medium facilitates the formation of new communities, social, cultural, political and economic interaction. The expansion of the Internet, the growth of search engines, and web pages and emergence of complex systems and behaviour could be viewed as displaying (semi) autopoietic patterns.[78] In his comprehensive study of the network society, Castells draws on some basic ideas of systems theory in his use of the metaphor of the space of flows to describe the process of meaning construction and the organisational logic of networks that are not dependent on functional and centralised hierarchical systems of ordering and control as such.[79] Castells does not however dissent from the view that the Internet is a medium populated by interdependent social actors as embodied in the:[80]

> *"…flows of capital, flows of information, flows of technology, flows of organizational interaction, flows of images, sounds, and symbols. Flows are not just one element of the social organization: they are the expression of processes,* dominating *our economic, political, and symbolic life. If such is the case, the material support of the dominant processes in our societies will be the ensemble of elements supporting such flows, and making materially possible their articulation in simultaneous time. Thus, I propose the idea that there is a new spatial form characteristic of social practices that dominate and shape the network society: the space of flows.* The space of flows is the material organization of time-sharing social practices that work through flows. *By flows I understand purposeful, repetitive, programmable sequences of exchange and interaction between physically disjointed positions held by social actors in the economic, political, and symbolic structures of society."*

The role of law in steering through social policies has now to accommodate the transformative effects of the Internet on the relational dynamics between the State and individuals in society on the one hand and the relationship between sub-systems on

[76] Ibid. at pp 7-8: "…the social construction of identity always takes place in a context marked by power relationships…a distinction [must be made] between three forms and origins of identity building: *Legitimating identity:* introduced by the dominant institutions of society to extend and rationalize their domination *vis a vis* social actors, a theme that is at the heart of Sennet's theory of authority and domination, but also fits with various theories of nationalism. *Resistance identity*: generated by those actors that are in positions/conditions devalued and/or stigmatised by the logic of domination, thus building trenches of resistance and survival on the basis of principles different from, or opposed to, those permeating the institutions of society, as Calhoun proposes when explaining the emergence of identity politics. *Project identity*: when social actors, on the basis of whichever cultural materials are available to them, build a new identity that redefines their position in society and, by so doing, seek the transformation of overall social structure."

[77] See B A Nardi and V L O'Day, *Information Ecologies* (Cambridge: MIT Press, 1997) and K Mossberger, C J Tolbert and M Stansbury, *Virtual Inequality, Beyond the Digital Divide* (Washington: Georgetown UP, 2003).

[78] P Bøgh Anderson, "WWW As a Self-Organising System", http://imv.au.dk/~pba/Homepagematerial/publicationfolder/WWWSelfOrg.pdf.

[79] M Castells, *supra* n70.

[80] Ibid. p 442.

the other.[81] Luhmann's conception of society as being constituted by communications, when transposed onto the Internet, underscores the complex tiers of information exchange, interaction and communication. Consider the reach of Luhmann's analysis of society and the resource potential of structural coupling in this highly interconnected environment in this observation by Benkler:[82]

> *"We live in a technological context in which a tremendous amount of excess capacity of the basic building blocks of our information and communication infrastructure is widely deployed. The widely distributed and topologically diverse deployment of these resources makes them ideally suited for building redundant, survivable backup systems for our basic information and communications infrastructure. Harnessing this excess capacity to create such a survivable infrastructure will likely be done most effectively, not through improving the ability to price these resources, but through improving the conditions for social sharing and exchange of the excess capacity users own. If we invest our policy efforts in hardening our systems to attack instead of rendering them survivable, if we ignore in our institutional design choices the effects on price-based markets and enterprise organization, we will lose a significant opportunity to improve the survivability of our information systems at relatively low cost and with minimal bureaucratic intervention."*

Luhmann's ideas of autopoesis and social systems may enable us to gain a better understanding of not only how the process of information sharing and exchange can take place but also the operable constraints that may prescribe the policy goals and objectives.

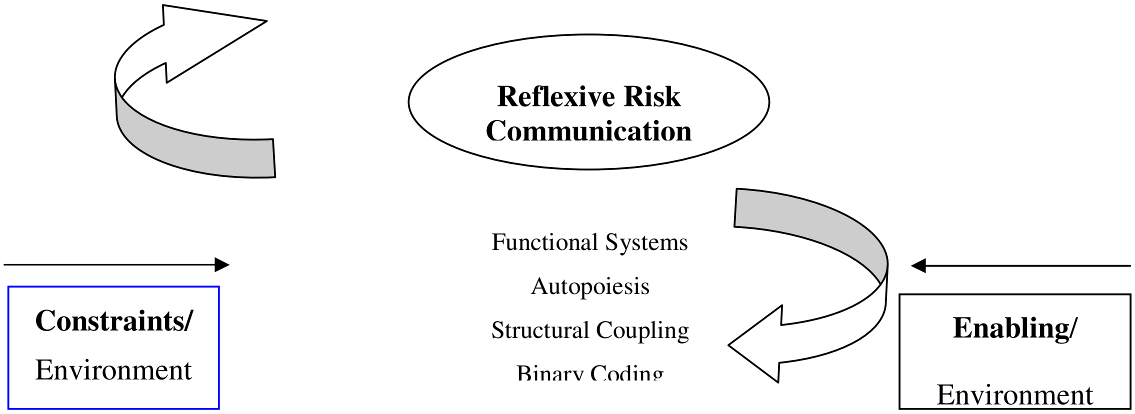
4.2 Application

A summary of some of the implications of Luhmann's insights for debates on the ability of the Fraud Act 2006 to manage political expectations about order and security in the online environment may be appropriate at this stage. We suggest that Luhmann's ideas about functionally differentiated and self-generating sub-systems when extended to identity theft have three specific implications for the way we can conceptualise and understand Internet governance. As argued previously, law is a necessary but not a sufficient governance instrument in managing the emerging threats on the Internet. The risks posed by identity theft are juridicalised – the illegal behaviour is identified and the outcome to such forms deviant behaviour is identified at the outset. The intention to derive a gain or cause a loss will now be sufficient. The political construction of risk is now interpreted by the courts and the institutions of enforcement through structural coupling. Second, phishing or identity theft is not a problem that law can solve – ultimately online criminal behaviour is a social not technologically driven problem. Notwithstanding the limits on the criminal law,

[81] Y Benkler, *The Wealth of Networks* (New Haven: Yale UP, 2006) p212, D R Johnson & D Post, "Law and Borders – The Rise of Law in Cyberspace", (1996) 48 Stanford Law Review 1367.

[82] Y Benkler, "Peer Production of Survivable Critical Infrastructures" in M Grady and F Parisi (eds), *The Law and Economics of Cybersecurity* (US: Cambridge, 2006) 73, 75.

Luhmann provides us with a framework that goes beyond the juridicalisation of identity theft. The third implication, we submit, is that emerging networks for information sharing, the evolution of specialised technological solutions and increased end-user participation is indicative of an important trend in the way online threats are conceptualised and managed.



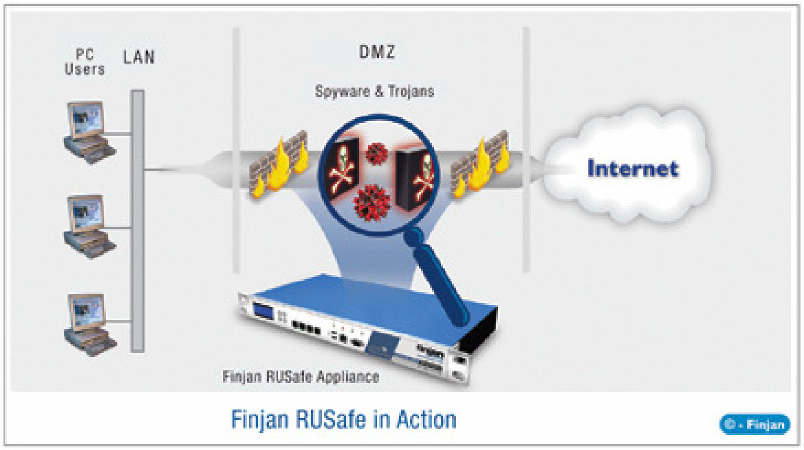
The central point here is that notwithstanding the limits faced by law in conceptualizing risks posed by identity theft or phishing attacks, we need to acknowledge the fact that other social systems and organisations can respond reflexively. Such a process enables society to transform itself, not in the sense of converting inputs into outputs, but through the autopoiesis of risk communications. In short, reflexive risk communications are producing functional systems and organisations that attempt to model complexity, security and system. Individuals, public and private actors can exist in different systems, organisations and can engage in interactions.[83] It is instructive to observe the way each sub-system reconstructs risk. For example, science is now assuming an important role in the light of political and legal communications and the constraints facing these systems in managing security threats. The emergence of new technological solutions and production of knowledge can in this respect be seen as a form of science coupling with law, politics education and economy. The market for information security is equally vibrant with a range of products relating to security and commercial operating systems.[84] VeriSign, for example, provides intrusion detection, threat scanning and patch implementation functions. Google, currently use web-crawlers to identify infected web pages. The process is akin to a form of data mining of infection vectors. Suspect URLs are visited and observed, with the aim of determining the malicious capabilities of these websites. Where a web site is shown to have malware binaries, the pages are marked

[83] See RAW Rhodes, "The New Governance: Governing Without Government", (1996) *Political Studies* XLIV: 652–67.

[84] See for example, "The Google Pack" collection of essential software at http://pack.google.com/intl/en/pack_installer.html?hl=en&gl=us.

as potentially harmful and displayed in search results.[85] Exploit Labs, for example provide LinkScanner functionality. Website owners can install a malicious content scanner on their site.[86] Visitors to the site can type or paste a URL into the LinkScanner text box and will know whether the web page is safe. If the link has potential malware binaries, the visitor will be informed of this. Another illustration of the growing trend of sub-systems responding to the constraints of law is the increased assimilation by these systems of 'ordering' values and norms.

Education and scientific systems are responding to the increased use of social engineering and malware infection techniques. These processes aim to provide a counterpoint to the methods employed by phishers and identity thieves in abusing trust.

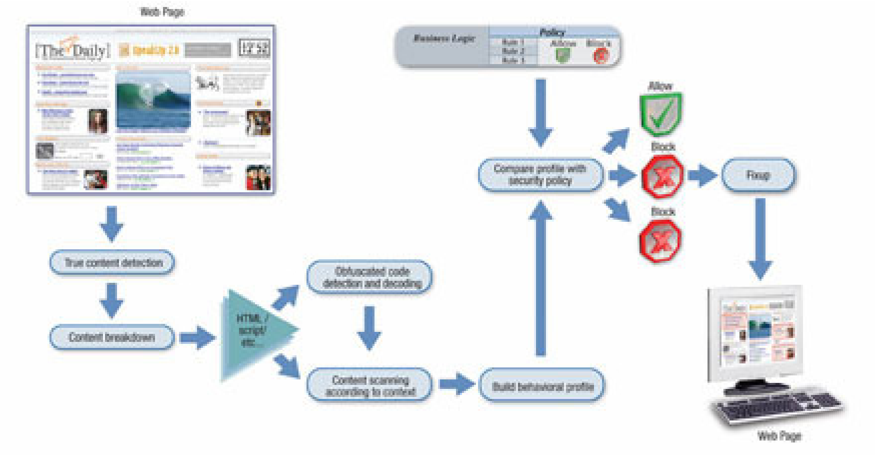


The use of "behaviour-based" technology helps minimise the threat consequences posed by the "gullible" human. For example, science reconstructs the decision making process that leads to risk exposure and puts in place the type of technology that independently undertakes an inspection of the application-level traffic and analyses the behaviour of suspect codes.[87] Organisations and individuals can now purchase secure gateway products to provide them with real time protection.

[85] M Lemley and B Hall, "The Law and Economics of Internet Norms", (1999) Berkeley Program in Law & Economics, Working Paper Series, University of California, Berkeley. Available at http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1131&context=blewp (accessed on April 4, 2007).

[86] http://www.explabs.com/LinkScanner/MyLinkScanner.

[87] http://www.finjan.com/content.aspx?id=190 .

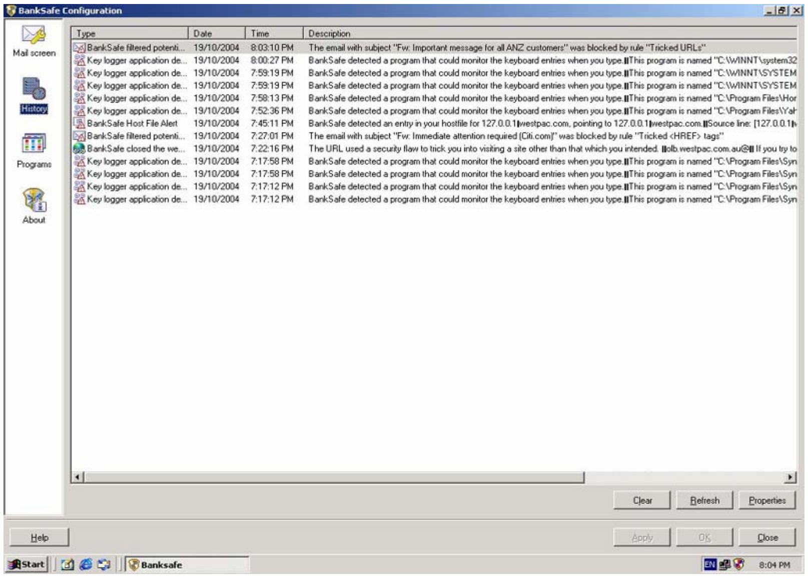


(www.finjan.com)

Additionally, software products now enable the identity of websites to be authenticated.[88] This software enables end users to determine whether the website they are visiting or accessed via an email link is a trusted site. The process of authentication is fairly straightforward. The user needs only to place the mouse over a logo or image and the verification software will highlight the trust credentials of the site. Given that the setting up of unique phishing websites is on the increase, this software aims to promote trust and confidence in end user being exploited by 'drive-by malware'. BankSafe is another commercial provider who has encoded 'risk management' norms into its anti-phishing software.[89] This software runs on Windows applications and provides real time protection. It scans web pages visited by the end user. For example, when the user visits a malware vector that steals passwords and usernames, the browser is instantly shut down. The software also provides an early warning detection facility when phishing emails arrive into the inbox or fake DNS entries detected.

[88] http://www.vengine.com/support/faq.html.

[89] http://www.smh.com.au/media/2004/10/22/1098316833157.html.



Type	Date	Time	Description
BankSafe filtered potenti...	19/10/2004	8:03:10 PM	The email with subject "Fw: Important message for all ANZ customers" was blocked by rule "Tricked URLs"
Key logger application de...	19/10/2004	8:00:27 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\WINNT\system32
Key logger application de...	19/10/2004	7:59:19 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\WINNT\SYSTEM
Key logger application de...	19/10/2004	7:59:19 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\WINNT\SYSTEM
Key logger application de...	19/10/2004	7:58:13 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\Program Files\Hor
Key logger application de...	19/10/2004	7:52:36 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\Program Files\Yah
BankSafe Host File Alert	19/10/2004	7:45:11 PM	BankSafe detected an entry in your hostfile for 127.0.0.1▮westpac.com, pointing to 127.0.0.1▮westpac.com.▮▮Source line: [127.0.0.1▮
BankSafe filtered potenti...	19/10/2004	7:27:01 PM	The email with subject "Fw: Immediate attention required (Citi.com)" was blocked by rule "Tricked <HREF> tags"
BankSafe closed the we...	19/10/2004	7:22:16 PM	The URL used a security flaw to trick you into visiting a site other than that which you intended. ▮▮olb.westpac.com.au@▮▮ If you try to
Key logger application de...	19/10/2004	7:17:58 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\Program Files\Syn
Key logger application de...	19/10/2004	7:17:58 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\Program Files\Syn
Key logger application de...	19/10/2004	7:17:12 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\Program Files\Syn
Key logger application de...	19/10/2004	7:17:12 PM	BankSafe detected a program that could monitor the keyboard entries when you type.▮▮This program is named "C:\Program Files\Syn

(www.smh.au)

The scientific communications are not only to be limited to commercial security software providers and standard setting organisations but also extend to spheres when individuals and organisations in society engage in communications about installing appropriate software and adopting Internet safety measures. ISPs for example, now educate subscribers and users on the importance of safe browsing. This initiative is an important response to malware writers increasingly targeting instant messaging and peer-to-peer networks as potential vectors for distribution of viruses and worms. Equally, commercial and non-commercial organisations now make available "safety packages" as part of their subscription, with regular information about security issues and updates for browsers, plugins, applications and operating systems.[90] For example, the Mozilla Foundation now makes phishing protection available on a non-commercial basis.[91] Visitors to the site are provided with a test site to see if the phishing protection facility on their system has been enabled. Microsoft also provides a range of information seeking to educate users on the type of phishing hoaxes.[92] These developments are in Luhmann's sense normatively closed autopoietic selections. These selections can be viewed as processes by which science and education synthesise information, utterance and comprehension. For the education system, knowledge about the threat landscape and risks are essential elements for decision making in organisations and individuals.

[90] M Lemley and B Hall, supra note 85. See also tips for cleaning and securing websites at www.stopbadware.org/home/security.

[91] http://www.mozilla.com/en-US/firefox/phishing-protection/.

[92] http://www.microsoft.com/protect/yourself/phishing/identify.mspx.

More generally, we cannot underestimate the valuable role played by non-State actors in using standards as a regulatory strategy. For example, the International Telecommunications Union (ITU) has been at the forefront of promoting transparency in the standardization process.[93] The European Telecommunications Standards Institute (ETSI) is another independent, non-profit organization, which continues to contribute to the creation of a culture of information security by developing telecommunications standards for technologies, which include telecommunications, broadcasting, intelligent transportation and medical electronics. The European Network and Information Security Agency, is another agency, which has directed its efforts in preventing, addressing and responding to information security issues.[94] Following the second phase of the World Summit on the Information Society (WSIS) in Tunis in 2005, the ITU acts as moderator of the WSIS Action Line C5 on building trust and security in the use of information and communication technologies.[95] The early indications are that these processes for information exchange and dissemination are providing avenues for structural coupling and sharing of knowledge and expertise.[96] Finally, the Convention on Cybercrime of the Council of Europe now makes available a binding international instrument on this particular subject.[97] This Convention provides a guideline, which countries can use to develop national legislation against Cybercrime and as a framework for international cooperation.[98]

5. Conclusion

This paper has sought to demonstrate that the Fraud Act 2006 facilitates the prosecution of identity theft and therefore makes a valuable contribution to Internet governance. That said, an overemphasis on the role of law can lead us to overlook the fact that the idea of absolute online security is a myth. Law may have some of the 'right answers'. Luhmann's ideas about functionally differentiated and autopoietic systems however, remind us that a deeper understanding of the reality of the threat landscape is a critical pre-requisite to information security policymaking. What is true of the processes and structures through which law conceptualises risk in the threat landscape is also true of other autopoietic sub-systems. Each sub-system conceptualises risk not with some universal or utopian goal but rather, with self-preservation in mind. Three observations may be offered by way of a conclusion. First, viewing society as a complex aggregate of systems that exhibit characteristics of

[93] http://www.itu.int/osg/csd/.

[94] http://www.enisa.europa.eu/rmra/h_home.html.

[95] See WSIS Action Line C5 and the Partnerships for Global Cybersecurity initiative

can be found at www.itu.int/pgc/, ITU Plenipotentiary Resolution 130: "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies" (Antalya, 2006).

http://www.itu.int/osg/spu/cybersecurity/pgc/2007/docs/security-related-extracts-pp-06.pdf ; http://www.itu.int/cybersecurity/.

[96] See ETSI, 2nd Security Workshop: Future Security 16-17 January 2007 - Sophia-Antipolis, France Workshop Report http://portal.etsi.org/securityworkshop/Presentations07/ETSI_2nd_Security_Workshop_Report.pdf

[97] The United Kingdom has yet to ratify the Convention.

[98] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

operational closure and open cognitive processes is timely – decentralised and distributed networks require an expansive view of governance. Second, as individuals can now belong to different subsystems (organisations) it becomes imperative that we seek creative ways through which online security spaces can be maintained. Third, we need to re-think how best questions about risk, responsibility and accountability can be structurally coupled with each other in a highly complex environment.