

On the Viability of Using Liability to Incentivise Internet Security

Huw Fryer^{1,2}, Roksana Moore², and Tim Chown³

¹Web Science Doctoral Training Centre, School of Electronics and Computer Science, University of Southampton,

²Institute for Law and the Web, School of Law, University of Southampton,

³Web and Internet Science, School of Electronics and Computer Science, University of Southampton,

June 3, 2013

Abstract

Internet use is characterised by externalities, which means that it can be sufficiently profitable for criminal enterprises to flourish. One possible mechanism which could be considered to improve incentives is liability. We conduct a review of the literature relating to liability theory, liability online, and security economics in general and consider the impact that liability on any particular group would have both to the group themselves and to the incentives of criminal groups. We conclude that although there are instances where liability could have positive economic effects or provide protection to consumers, as a purely economic mechanism its costs outweigh the benefits.

1 Introduction

A lot of the time, criminals are judgment-proof. They might reside in jurisdictions where the authorities are corrupt, consider cybercrime a low priority, or lack the technical knowledge to be able to do anything about it. Even in co-operative jurisdictions it can be difficult to gather enough evidence to successfully prosecute. Low reporting of cybercrime due to expense, man hours required, or reputational damage further decrease the risk (and therefore the deterrent) for criminals to participate in cybercrime¹.

Criminals are also able to take advantage of the fact that the Internet is characterised by economic phenomena which are characteristic of externalities and market failure which

¹NF Macewan, “The Computer Misuse Act 1990: lessons from its past and predictions for its future” (2008) 12 Criminal Law Review 955 .

lead to lack of incentive to preserve security. Security has the features of non-excludability (it is not possible to exclude the benefits of good security from others) and it is non-rivalrous (security by one does not diminish the availability for others) which means that it has public good features². As a consequence the free rider problem exists: it is better for everyone if everyone is secure, but since it's not possible to prevent others from enjoying the benefits of an individual's improved security then there is no incentive to take part in improving security as a whole³.

Information asymmetries also exist due to the gulf in knowledge between the average user and the vendors selling products. An example of this exists in commercial software⁴. Although a sufficiently expert user could check through the source code and satisfy themselves it was secure, such a task would be error-prone and take a considerable amount of time given that popular software can have millions of lines of code. In many cases, even this is not possible because the source code of the software is not made available and the license prohibits steps like decompilation⁵ to attempt to see how it works. A similar problem exists for ISPs as well, that the majority of users are not experts and cannot tell the difference between a secure or insecure ISP⁶. Akerlof's "market for lemons" becomes a reality in the market for both, with customers refusing to pay for a more secure version⁷ which leads competition focuses on price or features.

By changing the incentives, the externalities which exist can be internalised and force the actors involved to pay greater attention to security. There are many different actors involved whose actions unintentionally enable criminal enterprises to flourish: software with vulnerabilities, users with insecure machines, and operators of various bits of infrastructure such as ISPs, content and hosting providers. Since a lot of criminal activity relies on compromised machines⁸, it is this element which we focus on in this paper. Better secured machines on the Internet will force criminals to work harder and consequently introduce an additional direct cost to their enterprise and consequently reduce the profitability of cybercrime.

According to various theories about the purpose of liability, private law serves a function aside from the compensation of a victim in an individual case. Rather it also serves as a deterrent to certain types of behaviour or an incentive to take more care. This has been the case in the industrial world, but has not yet gained general acceptance as a

²Deirdre K Mulligan and Fred B Schneider, "Doctrine for Cybersecurity" (2011) 140(4) *Daedalus* 70

³Ross Anderson, "Why information security is hard-an economic perspective" in *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual* (2001).

⁴For a more detailed discussion of the problems of market failure in the software industry see Roksana Moore, "The role of standardisation in the raising of software quality [working title]" [2012] Pre-print

⁵Code which can be directly understood by a computer is converted from human readable source code through a process known as compiling. The reverse of this, to get the source code is known as decompilation

⁶Michael Van Eeten and others, "The role of internet service providers in botnet mitigation an empirical analysis based on spam data" in *Proceedings (online) of the 9th Workshop on Economics of Information Security, Cambridge, MA* (2010).

⁷Anderson, "Why information security is hard-an economic perspective" (n 3).

⁸Juan Caballero and others, "Measuring pay-per-install: The commoditization of malware distribution" in *USENIX Security Symposium* (2011).

mechanism in the virtual world. This paper analyses the effect of extending the application of these theories to the Internet with the hope of reducing negative externalities by deterring people from insecure behaviour through a financial penalty. At the same time, requiring criminals to work harder should introduce additional costs into their business model and hopefully discourage participation. We argue that there are many instances of externalities which could be adequately covered through imposing liability, but caution that there are several significant obstacles in the way and suggest that the carrot may be better than the stick in order to improve peoples' security behaviours online.

The remainder of this paper is structured as follows: Section 2 discusses related work of attempting to disrupt online criminal activity, and then the concept of liability in a general sense, and its application online. Section 3 begins with a scenario to illustrate the actors involved who might be the targets of liability. The actors from the scenario are then considered in terms of what externalities exist, and what impact liability would have if imposed on any of them. Section 4 looks at the problems in the way of using liability in general, in terms of practicality, cost and justice. We end with a conclusion that despite potential positive effects, significant obstacles exist with the use of civil liability as a means of improving security online and its use should therefore be discouraged.

2 Related Work

The majority of the literature and judicial activity has been in the USA, yet this paper is written from a UK perspective. USA law is persuasive, but not binding, on UK law, so principles can be carried across, even if the law is in some aspects very different. We do not intend to perform a comparative analysis of the two jurisdictions, but we will attempt to distinguish between the two, and occasionally provide context about the differences in individual instances where relevant.

2.1 Disrupting Cybercrime

There has been research in the past about targeting different parts of the cybercrime ecosystem for the best outcome. Caballero et al. studied the Pay Per Install (PPI) model used by criminals to infect computers, where affiliates get commission for compromising machines⁹. They suggested that the majority of the major malware families used PPI schemes, and given the comparatively low amount of PPI operators compared to the types of malware it could be a worthwhile area to target¹⁰.

Studies into spam have suggested that with such a low conversion rate it might also be vulnerable to economic targeting. Kanich et al. infiltrated the Storm botnet and redirected spam to domains they controlled with 350 million emails sent leading to 28 purchases (a conversion rate of less than 0.00001%). Extrapolation of the figures led them to conclude that the revenues are not that great and that a retail market of spam

⁹Caballero and others (n 8).

¹⁰ibid.

campaigns is not efficient enough to make a profit meaning that the only operators who can make a profit are groups such as the botmasters themselves¹¹. Levchenko et al. performed a comprehensive analysis of the entire spam value chain, and concluded that the area with the greatest potential for impact was that of the payment providers. The results indicated that just three banks provide 95% of all payment servicing and as such they represent a suitable bottleneck to target for a substantial impact in the profitability of spam. They suggest that were banks to refuse to settle transactions with banks identified as supporting spam then it could become infeasible for them to do so, which would represent a significant additional cost for spammers to correct¹².

Aside from payment providers, another financial aspect which has been considered has been the infrastructure which enables the criminals to physically transfer the money they make into their possession. In relation to banking fraud, money mules are one element which be considered a bottleneck for cybercrime. After transferring money from someone account, it is necessary to physically withdraw money from an account, so that it can be transferred into the destination account without it being linked to the crime, a process known as money laundering. Websites which recruit mules are recognised as being an important part of cybercrime, but whilst banks are aggressive in taking down phishing sites associated with their brand, they are less inclined to expend resources in targeting mule recruitment sites because the costs are shared between all banks and they don't know if doing so will help them or their competitors¹³. There has been news recently about the apparently co-ordinated takedown of Liberty Reserve, an anonymous currency exchange commonly used by criminals. It is too early to know the impact this will have on cybercrime, but it is expected to be significant¹⁴.

Botnets are a widely used tool for cybercrime, one approach has been to disrupt the operation of botnets as much as possible. A botnet is a network of computers (known as "bots" or "zombies") which are under the control of an external operator, usually through the installation of malicious software (malware). The bots perform any criminal acts such as distributed denial of service (DDoS) attacks against websites¹⁵, sending spam, or hosting illegal content¹⁶. Disruption of the botnet can take the form of either legal or technological measures, but will usually require analysis of botnet itself as a preliminary step, and the malware used to recruit bots to it, in order to search for structural

¹¹Chris Kanich and others, "Spamalytics: An empirical analysis of spam marketing conversion" in *Proceedings of the 15th ACM conference on Computer and communications security* (2008).

¹²Kirill Levchenko and others, "Click trajectories: End-to-end analysis of the spam value chain" in *Security and Privacy (SP), 2011 IEEE Symposium on* (2011).

¹³Tyler Moore and Richard Clayton, "The impact of incentives on notice and take-down" in *Managing Information Risk and the Economics of Security* (Springer 2009).

¹⁴Brian Krebs, "U.S. Government Seizes LibertyReserve.com" (28 May 2013) (<http://krebsonsecurity.com/2013/05/u-s-government-seizes-libertyreserve-com/>) accessed 2 June 2013.

¹⁵A denial of service attack (DoS) seeks to overwhelm a victim Web server, usually through an overwhelming volume of requests. It is unusual that a single machine can achieve this alone: a distributed DoS attack uses hundreds or thousands of computers to make it more difficult to distinguish from legitimate traffic and increase the strength of the attack

¹⁶On some occasions people have voluntarily joined botnets, or participated in DDoS attacks, for example Anonymous attacks in support of Wikileaks BBC, Anonymous Wikileaks supporters explain web attacks (Accessed 25 May 2013, 2011)

weaknesses or other means of disruption. One method is through the use of honeypots¹⁷, which not only gather intelligence, but arguably interferes with the criminals' economics as well since it introduces uncertainty into the criminal economy as it is impossible to tell which of the bots are real and which aren't¹⁸.

If the malware binary for any particular botnet is obtained, then the analysis can tell where the controlling (C & C) server is and how the bots communicate with it¹⁹. Researchers briefly managed to take over the Torpig botnet, by impersonating the C & C server²⁰ although that has since been upgraded to include improved cryptographic protection against this attack. A law based approach can be to buy all the known domains that the bots will contact in order to prevent the botmaster from communicating with them. This tactic was used with success against Srizbi and the notorious Conficker botnet. This can quickly become economically infeasible though, because the domains change regularly. A strategy known as "domain flux" has the bots attempt to communicate with every domain name on a list until it gives a response which identifies it as the C & C server. This means that to prevent communication every single one has to be bought, whereas the botmaster only needs to successfully communicate with one. In addition to financial cost, this is error prone and requires a huge amount of co-operation between different registries across different countries.

More recently, Microsoft has used legal injunctions to take over domain names and IP addresses of the C & C servers of a number of botnets including Waledac, Kelihos, Rustock and Zeus²¹. They were successfully able to argue that the botnets were doing damage to the reputation and goodwill of Microsoft's name because of spam received by Hotmail users and modifications made to the Windows kernel, and that the damage would likely continue without action²². This has had a moderate amount of success, global spam volumes dropped noticeably after the Rustock botnet was taken down²³. Unfortunately, whilst the botnet itself can't do anything itself the damage inflicted by the malware remains, since this might include silently disabling automatic updates. Therefore, these machines remain candidates to be re-recruited into another botnet and with the PPI system described above²⁴ the loss of a botnet is not a major issue for botmasters, since they can obtain a new one quickly and cheaply.

¹⁷A honeypot is a machine or server which is designed to look vulnerable to exploitation by the botnet malware. It can do this with varying degrees of interactivity: either simply collect the malware which is dropped, remain deliberately infected, or simply simulate a bot

¹⁸Zhen Li, Qi Liao, and Aaron Striegel, "Botnet Economics: Uncertainty Matters" in *Workshop on the Economics of Information Security (WEIS)* (2008).

¹⁹The C & C server is where bots get their instructions about which tasks to perform. It is commonly regarded as a weak point in botnet infrastructure, since eliminating communications can render the botnet harmless. Some botnets have got around this by adding additional layers of redundancy, such as direct peer to peer communication

²⁰Brett Stone-Gross and others, "Your botnet is my botnet: analysis of a botnet takeover" in *Proceedings of the 16th ACM conference on Computer and communications security* (2009).

²¹<http://www.microsoft.com/en-us/news/presskits/DCU/>

²²This strategy has continued to be used, the court documents can be seen at <http://noticeofpleadings.com>

²³Brian Krebs, Rustock Botnet Flatlined, Spam Volumes Plummet (Accessed 25 May 2013, 2011).

²⁴Caballero and others (n 8).

2.2 Theories of Liability

Tort law is private law between two parties where one will seek compensation from the other as redress for a wrong committed, and if the claimant is successful then the defendant pays compensation. Traditional tort theory held that this was the sole purpose of tort law. In early negligence cases, precedents were narrow in scope according to specific sets of facts. Restrictions were placed on who might be liable in terms of whether their behaviour specifically caused the specific accident²⁵. The textbook example of this is where a claim against a doctor failed for not treating arsenic poisoning because the victim would have died anyway, no matter how negligent he was²⁶. Despite this, it became apparent that the imposition of liability had more of an effect outside the instant case, and that additional rationalisation was required to explain them. The development of case law led to theorising about the function of tort law, or how it could be best used to achieve certain ends. A full discussion of the different theories is beyond the scope of this paper, but some of the major theories will be introduced here²⁷.

Enterprise Liability Theory is the idea that since the majority of cases in the industrialised world would form a certain case of inevitability, such as defective products or unpreventable workplace accidents. Tort law, being designed for individual accidents, was ill-suited to deal with the the new type of case. As a consequence, the compensation scheme does not fit into individual justice but rather in to a damages “lottery” where those who are fortunate enough to be able to prove that they were injured by a solvent party gained far in excess of what they required whereas others get nothing²⁸. Proponents of this theory of liability argue for the abolition of the tort law system, or failing that significant reform such that some form of need based damages can be provided to victims²⁹. Discussion of reform of the tort system has focused on product liability or other strict liability torts³⁰, and class action devices³¹ as a more equitable means of providing relief to victims. Enterprise liability theory also has notions of efficiency, that the enterprise is best placed to bear the risk because they can spread it through their customers and are best placed to act in response to the threat of liability³².

²⁵It would have to satisfy the “but for” test, which is to say that “the damage would not have occurred but for the defendant’s negligence”

²⁶*Barnett v Chelsea and Kensington Hospital Management Committee* (1969) 1 QB 428 .

²⁷a more detailed treatment is given in J Goldberg, “Twentieth Century Tort Theory” (2002) 90 *Georgetown Law Journal* , and the references within.

²⁸Patrick Atiyah, *The Damages Lottery* (Cambridge Univ Press 1997) p. 143-150.

²⁹The most notable instance of the abolition of a tort system was in New Zealand in 1974, where it was replaced by a social insurance scheme funded through contributions from motorists, employers and employees, and general taxation. The system provides compensation for personal injury regardless of fault. A detailed discussion of the Act from around the time of its enactment can be found in Donald Renshaw Harris, “Accident Compensation in New Zealand: A Comprehensive Insurance System” (1974) 37(4) *The Modern Law Review* 361

³⁰Robert L Rabin, “Some Thoughts on the Ideology of Enterprise Liability” (1996) 55 *Md. L. Rev.* 1190 , Focusing on the tort system in the USA, since that is the origin of much of the literature.

³¹John CP Goldberg, “Misconduct, Misfortune, and Just Compensation: Weinstein on Torts” [1997] *Columbia Law Review* 2034 .

³²George L Priest, “Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law, The” (1985) 14 *J. Legal Stud.* 461 .

Compensation deterrence theory evolved at roughly the same time as enterprise liability theory, and shared the view that traditional tort theory could no longer simply be an adjudication of individual cases. Rather, the individual cases became an opportunity for judges and juries to legislate on matters of social policy³³. This transforms the courts into a public law type of institution with cases acting as a merely

“A symbolic starting point for the allocation of financial responsibility that eventually works itself out in the world...”³⁴

. The remedies which can be provided within the tort framework are an injunction or compensatory damages, with the latter being far more common alongside a settlement outside of court. This being the case, the financial remedy provides a means to deter future conduct which the courts have decided to be socially unacceptable (through the use of an objective “reasonable person” standard) whilst at the same time providing redress for those who were the victims of the unacceptable behaviour.

Similarly, economic deterrence theory views all entities as rational actors, who will act in their own economic best interests. If an action they participate in causes problems to others in the area (for example smoke pollution), there they will continue to do so until some other cost forces them to. This is the purpose of compensation: a means of forcing actors to internalise costs which otherwise would have remained as externalities³⁵. By placing the required standard at an appropriate level, a socially optimal mix of precautions and accidents can be reached, beyond which the additional costs for precaution would outweigh the benefits society would gain from fewer accidents. This theory goes back to the well-known judgment of Learned Hand J in *United States v. Carroll Towing* where he held that the burden of the precaution should be equal to the value of the probability of an accident and the loss arising from it³⁶. The theory was popularised through Coase’s analysis of 19th century nuisance³⁷ law, and insight that as long as two parties know where the liability lies they will bargain for a socially efficient outcome³⁸. In the same paper, he argued that the decisions of judges in 19th century UK nuisance cases had consistently decided in favour of the most efficient outcome, a conclusion shared by Posner for 19th century US judges³⁹.

Using liability in this setting would require liability be imposed for the actions of another, which runs contrary to established law. Criminal events are usually regarded as “intervening acts” which break the chain of causation between the tortious act and the damage⁴⁰. A known exception is the relationship between employer and employee, where

³³Goldberg, “Twentieth Century Tort Theory” (n 27).

³⁴ibid citing American Law Institute’s Reporters’ Study.

³⁵William M Landes and Richard A Posner, “Positive Economic Theory of Tort Law, The” (1980) 15 Ga. L. Rev. 851 .

³⁶*United States v. Carroll Towing Co.* (1947) at 173, per Learned Hand J.

³⁷RH Coase, “Problem of Social Cost, The” (1960) 3 Jl & econ. 1 .

³⁸ibid.

³⁹RA Posner, “A theory of negligence” (1972) 1(1) *The Journal of Legal Studies* 29 .

⁴⁰There are a wider set of circumstances in certain states in the USA where this is allowed, including liability for selling alcohol to someone who is involved in a car accident, e.g. *Rappaport v Nichols* 156 A 2d 1 (1959). Other examples can be seen in D Lichtman and E Posner, “Holding Internet Service Providers Accountable” (2006) 14 Sup. Ct. Econ. Rev. 221

the employer is liable for acts committed by their employee during the course of their employment⁴¹. This is an area of the law with no satisfactory justification or rationale in the case law except that it works having grown from “*social convenience and rough justice*”⁴². Atiyah’s analysis of various existing rationales in the literature was that

*“it is simply the most convenient and efficient way of ensuring that persons injured in the course of business enterprises do not go uncompensated”*⁴³

. He contrasted the alternative of employees being liable and therefore demanding higher wages to pay for insurance policies, which would be considerably less efficient⁴⁴. The loss spreading argument is characteristic of enterprise liability theory, and has been used in courts⁴⁵. Principles of justice have also formed part of a rationale: firstly the deep pockets argument, that there should be someone solvent to be able to compensate the victim when ordinarily there wouldn’t be without it⁴⁶, and also that since it is the enterprise that makes money from risks to others it should be forced to accept the loss when it occurs⁴⁷. It has also been used specifically as an incentive to keep better control of their employees⁴⁸.

2.3 Liability

Lichtman and Posner suggested that the regulatory trend of ISP liability could not be justified on policy grounds, and instead liability should be imposed on ISPs for malicious traffic coming from their users in order to prevent insecurity⁴⁹. They argue that such liability is commonplace in areas where

*“liability will be predictively ineffective if directly applied to a class of bad actors yet there exists a class of related parties capable of controlling those bad actors or mitigating the damage they cause”*⁵⁰

They counter two common arguments against the imposition of liability that 1) ISPs will overreact and stop accepting risky users; and 2) ISP liability removes the incentive from users to take appropriate care. To the first, they argue that whilst some form of tax relief or support may be appropriate to assist smaller operators⁵¹ who may otherwise struggle to cope with the additional costs for litigation. To the second they argue that it

⁴¹*Lister v Hesley Hall Ltd* [2002] UKHL 22 , extended the principle for what constituted the course of employment to acts “so closely connected with his employment that it would be fair and just to hold the employers vicariously liable”.

⁴²*ICI v Shatwell* [1965] AC 656 , per Lord Pearce at 685.

⁴³Patrick Atiyah, *Vicarious Liability* (Butterworths London 1967) 26.

⁴⁴ibid.

⁴⁵*Various Claimants v Institute of the Brothers of the Christian Schools* [2010] EWCA 1106 .

⁴⁶*Limpus v London General Omnibus Company* [1862] H & C 526 , at 529, per Willes J.

⁴⁷*Dubai Aluminium v Salaam* (2002) 2 AC 366 , per Lord Millet at 21.

⁴⁸*Gravil v Carroll* [2008] ICR 1222 , at 26-27.

⁴⁹Lichtman and Posner (n 40).

⁵⁰ibid at 223. Vicarious liability in the USA extends beyond the employer/employee relationship, for example leaving keys in the car or selling liquor to someone who later drives and causes an accident so this is more closely analogous than the situation in the UK..

⁵¹ibid, 243.

is necessary to tailor the liability such that users retain the incentive to be secure. Given that transaction costs are low ISPs can use contract law to enforce conditions on the users⁵².

Johnson performed a detailed analysis on existing legislation and judicial opinion to examine the possibility of a tort for the victims of identity theft from cyber security failures by database operators⁵³. He concluded that general tort principles did support the idea that there was a relationship between the two parties (the victim and the database operator) so there was no reason in principle why liability could not be applied. Public policy would also support the notion of holding database operators liable, because losses would be minimised as a result of greater investment in database security. The rule prohibiting recovery for economic loss, a frequent stumbling block towards successful claims, should not apply to losses in regards to cyber security, but that claims should be limited so as to encourage operators to investigate for when a breach occurred so victims could take action. Since the paper was written however, there has been a considerable increase in the amount of US states with breach notification laws so this possibly does not apply to the same extent.

The issue of pure economic loss is one which has troubled the courts, and although in principle it has been recognised in certain narrow contexts, provided there is a sufficient “*assumption of responsibility*”⁵⁴ as being recoverable, courts are reluctant to award damages to the victims⁵⁵. A possible alternative method which could be considered in this context is damages for breach of privacy. The case law for this developed from old breach of confidence cases, and amongst the requirements is that information must have a “*necessary quality of confidence*”⁵⁶ at 419 per Megarry J., citing Greene M.R. *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 3 RPC 203, which is likely to implicitly be the case if the loss of the personal information can lead to financial loss for the victim. That said, there is no reason in principle why economic loss should be viewed as any different to physical loss, particularly with the Internet being such an important element of modern life.

Citron’s proposal also argued that the way we view property needs to change. However, the argument advanced was that negligence for database operators would be insufficient to cope with the problem for three main reasons⁵⁷. Firstly, the rapidly changing rate of technology means that it is difficult to know what the current optimal level of precaution to take would be, therefore leading to a potentially inefficient outcome. Secondly, there are no clear norms to guide for future behaviour because of the constantly evolving tactics of criminals making the idea of negligence “*shaky*” on its own⁵⁸. Finally, since there is a level

⁵²Lichtman and Posner (n 40) 244.

⁵³VR Johnson, “Cybersecurity, Identity Theft, and the Limits of Tort Liability” [2005] *beppress Legal Series* 713 .

⁵⁴*Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1963] AC 465 , at 529, per Lord Devlin.

⁵⁵The situation is different in the USA where most states do not permit recovery for economic loss alone, for fear of a virtually limitless liability

⁵⁶*Coco v AN Clark (Engineers) Limited* [1968] FSR 415

⁵⁷DK Citron, “Reservoirs of danger: The evolution of public and private law at the dawn of the information age” (2006) 80 S. Cal. L. Rev. 241 , 265.

⁵⁸*ibid* at 268, citing Kenneth S Abraham, *The forms and functions of tort law: an analytical primer on cases and concepts* (foundation Press 1997)

of residual risk of data leakage in any event, strict liability should be used to discourage marginal operators from entering the market, and efficiently allocating the risks⁵⁹. As such, the courts should adopt a *Rylands v Fletcher*⁶⁰ strict liability model. The databases used to store personal information were argued to be an analogy to the reservoirs of the 19th century, and that the natural consequence of the “escape” of personal data is identity theft, or harm for the victims⁶¹.

That negligence may prove problematic in keeping with the state of the art does have some support. The “commercial reasonableness” requirement for the security procedures in commercial funds transfers⁶² was recently tested in *Patco Construction v Ocean Bank*, and no useful guidance as to current norms or future standards was provided. The only guidance to emerge was that security procedures used by the bank in 2009 (based on guidance from 2005⁶³) were not commercially reasonable.

The providers of software have also been the target on several occasions, Microsoft in particular due to its huge market share and the global impact vulnerabilities in its software has⁶⁴. Holding developers liable was central to Rustad and Koenig’s proposal of a tort for “negligent enablement of cybercrime” based on product liability⁶⁵. The proposal is that providers of services and products used on the Internet be liable for knowingly marketing defective products and services. This they argued is much like the producers of cars, whose products became noticeably safer and more secure once they were the subject of product liability. Security expert Bruce Schneier has been a proponent of liability for software vendors, arguing

“Software vendors are in the best position to improve software security; they have the capability. But, unfortunately, they don’t have much interest”⁶⁶.

The report by Anderson et al. report for the European Network and Information Security Agency (ENISA) considers several of these issues in the liability section of their report. They rejected the notion of liability for ISPs in favour of a scale of fixed statutory damages for damages of any malicious users, because of its ability to continue to provide a deterrent

⁵⁹Citron (n 57) 267.

⁶⁰*Rylands v Fletcher* (1868) 3 HL 330, was a 19th century case concerning the escape of water from a reservoir where the court held that the defendant was strictly liable for any damage caused by “non-natural” use of land.

⁶¹The notion of a computer/land analogy has been discussed as well in the context of cybertrespass (RA Epstein, “Cybertrespass” [2003] 70[1] *The University of Chicago Law Review* 73). This was largely in response to the decisions in *eBay v. Bidder’s Edge* (*eBay, Inc v Bidder’s Edge, Inc* No. C-99-21200RMW, [2000] 100 F Supp 2d 1058) and *Hamidi v. Intel*. This revolves around whether a computer is sufficiently analogous to land (and hence not requiring actual damage) as opposed to chattels (where actual damage would be required). A discussion of trespass is beyond the scope of this paper.

⁶²The UCC specifically discounts negligence from applying, but the principle remains the same. Because liability is not strict, then an objective determination has to be made as to the level of care taken. UCC 4A-202(b)

⁶³FFIE C, “Authentication in an internet banking environment (2005)” (2005) (<http://www.fdic.gov/news/news/financial/2005/fil10305.html>) accessed 3 January 2012.

⁶⁴e.g. Emily Kuwahara, “Torts v. Contracts: Can Microsoft Be Held Liable to Home Consumers For Its Security Flaws?” (2007) 80 S. Cal. L. Rev. 997

⁶⁵ML Rustad and TH Koenig, “Tort of Negligent Enablement of Cybercrime, The” (2005) 20 *Berkeley Tech. LJ* 1553

⁶⁶Bruce Schneier, “Information Security and Externalities” (2007) 2(4) *ENISA Quarterly* 3

whilst simplifying the liability when it occurred. In relation to liability for defective software, it was suggested that a simple approach might have worked in the past, there are too many products which have use software for an approach like this to be viable as an overall solution⁶⁷. Instead, they recommend that vendors be liable for vulnerabilities in order to encourage an improved rate of patching.

That users might be subject to liability is also an issue which has been considered. Henderson suggested that a zombie computer which was “*knowingly insecure in the face of a well-known threat*”⁶⁸ could be considered negligent, describing it as akin to driving a car on the road with a known defect. It was suggested that, with the threat of lawsuits, the ordinary level of care taken by users would evolve into a level of care sufficient to make DDoS attacks less practical. The notion of duty was considered in response to the costs incurred by the actions of “Mafiaboy” in February 2000, as a means for the victims to obtain damages from someone solvent in a manner similar to the manufacturers of firearms for victims of their use⁶⁹. De Guzman by contrast considered liability a means of forcing users to internalise the costs of their own insecurity. It was suggested that finding liable someone who left the keys in a car door for damage when the car got stolen could be extended to leaving a home computer unsecured⁷⁰. The analogy was further extended, that whilst a stolen car didn’t have the owner present, a hijacked computer did and as such was similar to a car on the road with a consequent duty to other users⁷¹.

3 Using Liability for Information Security

In this section we set out a scenario, and then go through the externalities which exist for each actor and the effects of imposing liability, followed by a general discussion of liability in general. The following discussion is made with a few assumptions: first, we assume that it is possible to claim damages for economic loss, and that tort based liability does not have restrictions in using liability in this context⁷². In addition, we assume that the case law concerning safe harbour clauses for intermediaries can be reconciled with limited liability for them⁷³. Finally, we assume that every single actor concerned is subject to

⁶⁷Ross Anderson and others, “Security economics and european policy” [2009] 55 .

⁶⁸Stephen E Henderson and Matthew E Yarbrough, “Suing the Insecure?: A Duty of Care in Cyberspace” (2002) 32 New Mexico Law Review 11 .

⁶⁹ibid at 16.

⁷⁰T Luis De Guzman, “Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges” (2009) 59 Cath. UL Rev. 527 .

⁷¹ibid, at 555.

⁷²Several things may prevent the successful operation of tort in this area. In particular, it is against the authority of *Perl v CamdenPerl (Exporters) Ltd v Camden London Borough Council* (1983) 1 QB 342 that criminal acts are an intervening act. Causation and reasonable foreseeability could also pose problems: “but-for” causation requires that a negligent act specifically caused the damage(n 26), and that the act could cause some damage in particular. This will often be difficult (though not impossible) to prove, given the amount of malware which exists, and blame amongst many different parties.

⁷³In the UK, intermediary liability is governed by the EC E-Commerce Directive Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L178/1. The Google AdWords case, Case *Google France SARL v Louis Vuitton Malletier SA* (2010) 2010 ECR I emphasised

UK law⁷⁴.

3.1 The Actors Involved

The scenario begins with Alice who uses a search engine to find trusted site `http://bob.example.com` which has been hacked and infects her computer with malware through vulnerability in a popular browser plugin. Bob's site was compromised through a vulnerability in the popular CMS software he was using, which had been patched the week before but Bob had failed to update it. Unaware that her computer is infected and has started communicating with a C & C server (hosted by Mallory Hosting Ltd.), she continues browsing the Web as normal whilst in the background her computer starts performing criminal acts without her consent. She infects Charles who is on her network and both computers participate in a DDoS attack against Diane, with the botmaster taking advantage of the fact that their ISP has not implemented BCP 38⁷⁵ and that Bob is running an open recursive DNS server⁷⁶

3.2 The Externalities

Frequently, it is bugs in software which are exploited and enable the compromise of the end-user's device. This is one of the major examples of the failure of the market to sufficiently incentivise Internet security. From the point of view of a software vendor, there are significant commercial advantages to being the first entry in the market: proprietary formats and training costs for switching between different products encourage lock-in to both personal and business users⁷⁷. Users appreciate bug fixes or other improvements, but they are unlikely to notice any security features which minimises the incentive to work on them. Whilst these companies make profit from their product, there are additional costs incurred by their users and the Internet as a whole from the flaws in it. The MS08-067 bug which was exploited by Conficker, amongst others, cost £millions in damages⁷⁸.

Similar externalities exist for websites who affect the same group of people, but in slightly different ways. A site could be compromised in two main ways: it could serve malware to its visitors or its database could be compromised leading to loss of confidential customer

that a search engine was entitled to the immunity as long as its dealing with the information did not constitute actual knowledge of its illegal nature even if it was being paid to advertise, and Case C-277 *Scarlet Extended SA v SABAM* (2012) 2012 ECDR reinforced that an ISP could not be made to generally monitor all communications of its customers, even to search for instances of illegally downloaded content.

⁷⁴The UK population represents only a small fraction of Internet users, so the effect might be limited in real terms

⁷⁵Paul Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing" [2000] See discussion on page 14

⁷⁶The Domain Name System (DNS) is a service which maps the user friendly domain names like `www.example.com`, to IP addresses which computers can understand. See further discussion below on page 14

⁷⁷Anderson, "Why information security is hard-an economic perspective" (n 3).

⁷⁸or even £billions if some reports are to be believed, Dancho Danchev, Conficker's estimated economic cost? \$9.1 billion (Accessed 25 May 2013, 2009)

information. Malware is designed to be stealthy, so users can't link the fact that they had malware to the visit of a particular site. Breach notification laws exist so whilst there may be some indirect costs for the website through bad publicity, the victim potentially faces a large amount of work to reclaim their identity or get back any financial loss from the breach.

Many web applications are based around user generated content, which significantly increases the risk of malicious users spreading malware or running phishing scams amongst other things. Other services by their very nature carry a risk. Search engines list billions of websites and hosting providers provide web space and bandwidth to many websites, which may or may not be malicious. There is very little incentive for any of these actors to check the content, because it is time consuming, error prone, and expensive. These groups are also generally protected with immunity from liability⁷⁹.

ISPs have externalities in two ways. They could identify compromised machines in their space, and have a remediation policy to prevent future attacks. This (usually) doesn't happen, because relative to the profits that they might make per subscriber, the cost of a remediation policy is quite high in terms of infrastructure and support costs. Because users cannot tell which ISP is more secure, competition is fought on price, which makes it even more difficult to spare the resources. There are also justified fears about what would happen if they made a mistake and took action against a certain subscriber. This would inconvenience the subscriber, and consequently cost the ISP money, and possibly even lead to legal action.

Finally, there are significant externalities from users which cause insecurity. Users place a low economic value on their machine, and malware is designed to be barely noticeable to the victim whilst causing problems to everyone else. Other studies have demonstrated the low economic value users place on their computer security or privacy as long as there is a perceived benefit for them. Christin et al.⁸⁰ and Kanich et al.⁸¹ both ran studies on the crowdsourcing tool "Mechanical Turk"⁸², which allows companies to offer to pay users a small amount of money to complete tasks easily accomplished by humans but difficult for computers to do. Both studies asked users to install untrusted programs on their computer for amounts as little as \$0.01 and found a significant percentage were prepared to do so⁸³. Even a user with a higher economic value on their computer it would not necessarily be advantageous to be security conscious. Installing anti-virus software on a computer slows it down, and a user who patches their software uses bandwidth for no noticeable benefits. In fact, insecure behaviour could have a positive outcome for them. File sharing allows a user to get software which is either illegal in their country, prohibitively expensive, or simply more than they are prepared to pay, and they are able

⁷⁹See footnote 73

⁸⁰Nicolas Christin and others, "It's all about the Benjamins: An empirical study on incentivizing users to ignore security advice" [2012] 16 .

⁸¹Chris Kanich, Stephen Checkoway, and Keaton Mowery, "Putting out a hit: crowdsourcing malware installs" in *Proceedings of the 5th USENIX Workshop on Offensive Technologies* (2011).

⁸²<https://www.mturk.com/mturk/welcome>

⁸³The program was not malicious but did scan the process lists for evidence of malware. Interestingly, they found that there was a positive correlation between an anti-virus program and malware on the computer

to use it for free whilst not being noticeably affected by additional things the software might be doing. Individual losses are unlikely even if they do fall victim to cybercrime. Herley observed that by spending more than 0.36 seconds a day checking links to see if an email is a phishing email then an individual user will lose more in lost time over a year than they would if they fell victim a phishing attack⁸⁴!

The DDoS attack from the scenario is known as a DNS reflection or DNS amplification attack, and is an example of how the externalities together can provide bad security for a blameless party. It works by the attacking computers (Alice and Charles) making a DNS request of a large record, but “spoofing” their source IP address. Bob’s open recursive DNS server will provide an authoritative response to any computer which requests it, and the requests by Alice and Charles to Bob appear to be from Diane. As such, Diane’s server is bombarded with a lot of responses to requests it never made. The amount of computers involved means that a lot of queries can be executed simultaneously. The DNS server increases the size of the response approximately 60 times compared to the request. The large amount of open recursive DNS servers on the Internet⁸⁵ means that limiting requests from a certain source is not practical, because the zombies can simply use another DNS server. Similarly the victim cannot blacklist every DNS server which is sending them responses, because they themselves will want to use DNS. The fact that it is possible to spoof source IP addresses is what makes the attack possible, and it is this which BCP 38 attempts to prevent by mandating that network operators drop packets with spoofed source IP addresses. On the edge of a network, it is possible to tell if a source IP address is from outside the network and therefore easy to drop, but once the IP packet is outside of the network it is considerably more difficult to do so reliably.

3.3 Discussion

Software vendors have often been considered as a target for liability when the software vulnerabilities lead to losses. Intuitively, this makes sense: flaws in the software are often the direct cause of the successful compromise of a computer. As the complexity of software increases, the amount of defects in code increases. In order to minimise the risks and make the vulnerabilities more difficult for the attackers to find, a rigorous testing procedure is required, and a rational software company will only test as long as the costs of bugs outweigh the costs of testing the product⁸⁶. With the costs of litigation, the incentive to spend more time testing, and consequently create a more secure product is increased. Both deterrence theories support this notion, because the financial penalty shifts the incentive towards making a more secure product. The software vendor is better situated than the users to internalise the costs, and also in possession of the requisite knowledge and expertise to correct the flaws so can be justified under enterprise liability theory as well.

⁸⁴Cormac Herley, “So Long, and No Thanks for the Externalities” in *Workshop on New Security Paradigms Workshop (NSPW)* (2009).

⁸⁵The open resolver project <http://openresolverproject.org/> estimates there are 25 million open recursive DNS servers which pose a significant threat. Last accessed 25 May 2013

⁸⁶Ross Anderson, “Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore” [2002] at *Open Source Software Economics* .

The increased effort does not necessarily represent an optimal level of precaution, however. As the size of the codebase increases, so too does the probability that the vulnerabilities discovered by the developers are different to ones discovered by criminals⁸⁷, meaning that the impact of their additional effort is minimal. The increased level of care to avoid litigation passes additional costs on to the customer which could lead to the creation of an unintended side-effect: if the cost of the product increases to protect against liability, then it is possible that a greater number of users will seek to pirate it. This is an additional vector for malware infection, because there is no way for the user to check that this the pirated product doesn't contain malware. Even if it doesn't, users who do choose to use pirated software will not get security updates, and therefore make themselves vulnerable to exploitation in the future.

An alternative, as discussed on page 11, is to simply impose liability for losses caused for known vulnerabilities whilst a patch is unavailable⁸⁸. This solution is a lot more realistic, and could improve the rate at which software companies respond to reported vulnerabilities rather than risk liability. It should also be noted that it appears that the major software companies are generally doing a good job of patching security holes but not enough users install the patches. This can be seen from the small amount of zero-day attacks (18) identified by Bilge & Dumitras⁸⁹ from 2008-2011 and the small amount of hosts targeted. Contrast this with the most popular exploit attempts 3.3, taken from the Microsoft Security Intelligence Report for the second half of 2012⁹⁰. Aside from a couple of Java exploits, every other attempt targeted vulnerabilities which were patched several months, if not years before. The most common was malware identified as Win32/Pdfjsc which targets JavaScript execution vulnerabilities in Adobe Reader software. The latest vulnerability known to be targeted was CVE-2010-4091 which was patched on November 16 2010. Even for more recently patched vulnerabilities, it takes several months for a large increase in exploit attempts. CVE-2011-3544, a Windows vulnerability patched in December 2011, had only 132 exploit attempts in the first three quarters jumping to 199,648 in the fourth quarter. The most common Flash vulnerability to be targeted was CVE-2007-0071 - patched in 2008!

This calls into question the impact of liability on software vendors would have, since the figures suggest that users don't adequately patch the software running on their computers. If users patched adequately, there would be little point in attempting to exploit those vulnerabilities as has clearly been the case. Research by Skype supports this notion, suggesting that some 40% of users don't patch their computers adequately⁹¹.

Websites are arguably both a specialised class of user, as well as a specialised class of software vendor. They need to patch the software they are running on their server and

⁸⁷anderson2001

⁸⁸Anderson and others, "Security economics and european policy" (n 67).

⁸⁹Leyla Bilge and Tudor Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world" in *Proceedings of the 2012 ACM conference on Computer and communications security* (2012).

⁹⁰Danielle Alyias (Microsoft) and others, *Microsoft Security Intelligence Report, Volume 14* (techspace rep, Technical Report 2013) .

⁹¹Skype, "Survey Finds Nearly Half of Consumers Fail to Upgrade Software Regularly and one Quarter of Consumers Don't Know why to Update Software" (23 July 2012) (http://about.skype.com/press/2012/07/survey_finds_nearly_half_fail_to_upgrade.html) accessed 5 March 2013.

Exploit	Platform or technology	1Q12	2Q12	3Q12	4Q12
Win32/Pdfjsc*	Documents	1,430,448	1,217,348	1,187,265	2,757,703
Blacole	HTML/JavaScript	3,154,826	2,793,451	2,464,172	2,381,275
CVE-2012-1723*	Java	–	–	110,529	1,430,501
Malicious IFrame	HTML/JavaScript	950,347	812,470	567,014	1,017,351
CVE-2010-2568 (MS10-046)	Operating system	726,797	783,013	791,520	1,001,053
CVE-2012-0507*	Java	205,613	1,494,074	270,894	220,780
CVE-2011-3402 (MS11-087)	Operating System	42	24	66	199,648
CVE-2011-3544*	Java	1,358,266	803,053	149,487	116,441
ShellCode*	Shell code	105,479	145,352	120,862	73,615
JS/Phoex	Java	274,811	232,773	201,423	25,546

Table 1: Reproduced from Microsoft Security Report July - December 2012. *Vulnerability also used by the Blacole kit, the totals for this vulnerability exclude Blacole detections

conduct due diligence in order to avoid being compromised, whilst at the same time they need to keep their own code up to date. Websites require the use of additional software to keep running, the main two being the Web server and the database. Another commonly used piece of software is content management system (CMS) software which allows novice users to add content to a website without any programming experience, and “plugins” which can be placed on a site to perform common bits of functionality. Like other software, these have bugs and vulnerabilities which are patched as they are discovered, so a website which keeps these unpatched has an increased risk of attack. Similarly, poor quality code of their own also opens the site up to compromise whether through attacks on their clients (e.g. cross site scripting (XSS) to redirect a user to a page impersonating the real page), or their own server (e.g. SQL injection).

Unlike software, which is often dominated by a few large companies, websites can be created by anyone, and it is this low barrier to entry which has helped to make the Internet so popular. Whilst big, popular websites have been known to be successfully attacked⁹², and will often be run by large companies, on many occasions it will be a smaller website run by volunteers without any security expertise, or resources to pay damages which makes the loss spreading argument less persuasive.

If strict liability were to be introduced as Citron suggests⁹³, then this could have the effect of deterring the creation of websites and data collection by people who aren’t qualified to maintain them properly. This may have a positive effect on security, both for preventing malware propagation and losses from data breaches. Many websites which are used for hosting phishing pages are compromised more than once⁹⁴, and the sheer amount of websites makes even a small percentage of insecure sites a potential problem. For example, the latest Netcraft Web survey suggests that there are 672,837,096 sites on the Web⁹⁵. WordPress is said to have a market share of 17.9% of them, and of

⁹²For example LinkedIn was breached in June 2012 and 6.5 million passwords were leaked, see BBC, “LinkedIn passwords leaked by hackers” (6 July 2012).

⁹³Citron (n 57).

⁹⁴Tyler Moore and Richard Clayton, “Evil searching: Compromise and recompromise of internet hosts for phishing” in *Financial Cryptography and Data Security* (Springer 2009).

⁹⁵Netcraft, “May 2013 Web Server Survey” (3 May 2013) (<http://news.netcraft.com/archives/2013/05/03/may-2013-web-server-survey.html>) accessed 3 June 2013.

those 2.8% are using one of the version 2 releases⁹⁶. Security releases have been released since⁹⁷, which means that there are some 33 million WordPress sites with known “critical” vulnerabilities⁹⁸.

At present, it might be that the strategy of criminals is to compromise websites and use them for hosting illegal content, but this is not the only way. For example, zombie machines could host whatever the desired content, and simply register domains, much like the Avalanche phishing group did⁹⁹. Raising the bar too high for new entrants could also have the problem of inhibiting free speech for legitimate users, or pose additional costs for new entrants seeking to enter a market and thereby inhibit competition.

Users are frequently regarded by the security community as the root of all problems: they click on links to dodgy websites, don’t patch their machines, and use the same, simple, password for every account they use. This is not necessarily their fault, and in many cases is not fair. There are rational reasons for not wishing to patch a machine, such as stability, bandwidth costs, and not wishing to install the additional “features” on offer¹⁰⁰. Complicated password management strategies offer no noticeable security benefits for users either¹⁰¹. Nevertheless, users represent a significant factor in enabling cybercrime, even if only in a contributory negligence sense. Without some means to incentivise users to change their behaviour, any efforts against other groups will have a limited effect, so we turn to consider liability against users.

Although it may be considered harsh to impose liability on users, especially if the user isn’t very computer literate, yet negligence principles hold an objectively reasonable standard of behaviour, regardless of whether or not the person has the capacity to do better. The case establishing this concerned a learner driver who caused an accident: the court held that “*her incompetent best was not good enough*”¹⁰² and that she was therefore negligent. Although the consequences of incompetent drivers on the road are considerably more serious than incompetent users of the Internet, if we care about the damage that they can cause to others rather than themselves then it is an analogous situation.

Academic research has generally avoided considering liability on users for insecurity, and where it has, it has done so as a concept rather than a detailed consideration of the practical effect¹⁰³. It is possible that compensation deterrence theory could offer some support to the notion, since it is about the courts’ rulings on what they consider to be socially acceptable standards of behaviour. Requiring users to have the latest version of software, anti-virus and to act in response to notification that their computer is compro-

⁹⁶w3techs com, “Usage statistics and market share of WordPress for websites” (<http://w3techs.com/technologies/details/cm-wordpress/all/all>) accessed 3 June 2013.

⁹⁷WordPress, “3.0.4 Important Security Update” (29 December 2010) (<http://wordpress.org/news/2010/12/3-0-4-update/>) accessed 3 June 2013.

⁹⁸This is not to say that WordPress is any less secure than any other CMS system, merely that it powers a huge amount of the Web and as such the impact is more noticeable

⁹⁹apwg

¹⁰⁰See section 5.5 of Anderson and others, “Security economics and european policy” (n 67) for the challenges about patching.

¹⁰¹Herley (n 84).

¹⁰²*Nettleship v Weston* (1971) 2 QB 691 .

¹⁰³De Guzman (n 70), Henderson and Yarbrough (n 68)

mised could be considered desirable norms to aim for. However, the economic arguments generally fail: they are difficult to identify, less likely to be solvent, and the expenditure in effort for them to reach what might be considered an objective standard is incredibly high¹⁰⁴, which suggests that liability is probably not appropriate.

3.4 Shifting the Blame

As the discussion so far has shown, there will be occasions where it is difficult to identify the negligent party, or if they are identified they do not have resources to make good the loss. If it is not appropriate to impose liability on the groups discussed above, then the intermediaries who are in a position to control their behaviour should be considered. From our scenario, there are several intermediaries: Alice's ISP; Bob's hosting provider, (Mallory Hosting); and the search engine Alice used.

The advantage of liability for these groups is that they are in a much better situation to take action than their customers, because it requires action and knowledge by only one group rather than many. ISPs can take remedial steps on behalf of their users, through warning or more direct methods¹⁰⁵. A hosting provider running a single server with multiple users can roll out the updates as it gets them as opposed to every website having to update the software of their servers. A social media site or search engine checking the danger of the links on its site takes far less effort than every user checking individually. They are also an identifiable enterprise, probably with more resources than the negligent party themselves, which ensures that victims have some means of redress in the event of harm. Even in the event that liability were not considered for these groups, it would be necessary for any legal proceedings to attempt to identify the parties involved¹⁰⁶.

ISPs are a key element of any strategy for ensuring an overall good level of Internet security, because they can see when users connect to botnet C & C servers or participate in DDoS attacks. There is a distinct difference as well between good and bad ISPs, with van Eeten et al.'s analysis of a spam trap finding that 50% of spam can be attributed to just 50 ISPs¹⁰⁷. Research by Moura supports the notion that one compromised machine increases the likelihood that machines in the same subnet will also be compromised, what they called "bad neighbourhoods" of malware¹⁰⁸. ISPs could remediate the machines which they know to be compromised which could range from a simple notification by email or browser pop-up with instructions on how to remove the malware from the computer

¹⁰⁴Herley discusses the expenditure of time and effort of normal users against the benefits (both perceived and actual) that they get, Herley (n 84).

¹⁰⁵Anderson and others, "Security economics and european policy" (n 67).

¹⁰⁶Of course, this is not fool proof. Criminals can use stolen credit cards to use an identity, and even websites with an interest in knowing the real identity of their users get it wrong occasionally, see Dominic Rushe, "Facebook share price slumps below \$20 amid fake account flap" (3 August 2012) (<http://www.guardian.co.uk/technology/2012/aug/02/facebook-share-price-slumps-20-dollars>) accessed 27 May 2013

¹⁰⁷Van Eeten and others (n 6).

¹⁰⁸GC Moreira Moura, "Internet Bad Neighbourhoods" (University of Twente 2013).

right up to quarantining from the network. These steps all have limitations¹⁰⁹, in terms of impact (a user is not guaranteed to respond¹¹⁰) or support costs¹¹¹.

As Lichtman and Posner suggest, transaction costs are low between an intermediary and their customers¹¹², and as such they are in a position to enforce certain standards from their customers. Hosting providers and ISPs, for example, could contract with their users that they submit their machines to posture checks or that they agree to accept liability should they not be using the latest version of software. Anderson et al., suggest that ISPs should quarantine infected machines as soon as notified, but suggest allowing the user to un-quarantine the device as long as they accept liability¹¹³. They raise the concern that the ISP might become too defensive and begin to quarantine machines before verifying whether or not they are compromised¹¹⁴, and this is a potential issue for all of the intermediaries discussed. A hosting provider would need to verify the websites it was hosting were compromised or malicious¹¹⁵, because false positives are inevitable. Were they to be liable for everyone who visited a compromised website they hosted whilst they were verifying reports then they might be tempted just to shut it down prematurely rather than risk the expense¹¹⁶. Scale could also pose a problem for ISPs, since it would be necessary to verify any reports, with a lower bound estimate of 5% of all devices worldwide are infected, the resources it would take to successfully remediate them all could be significant¹¹⁷.

The hosting providers, ISPs and websites driven by user content are obvious examples of secondary liability. By providing a service, should they be liable for how people use it? In each case, they have low transaction costs with their users and can enforce certain standards of behaviour, yet as the analysis of vicarious liability has emphasised, there is the potential for “rough justice”¹¹⁸. This is an important consideration (in circumstances of both vicarious and direct liability), especially due to the variety of classes of potential defendant. Whilst a lot of money is made on the Web, a lot of operators are not particularly big or don’t make very much. With limited resources, it is incredibly difficult to keep up with the latest threats and completely defend against them. Larger operators are faced with a scale problem, and the unpredictability of users makes it impossible to completely prevent security lapses. These situations also limit the

¹⁰⁹Recommendations for the Remediation of Bots in ISP Networks (RFC 6561 available at <http://tools.ietf.org/html/rfc6561>, March 2012) (RFC6561).

¹¹⁰Or believe for that matter that they have to go to a certain website and download .exe files to fix their computer

¹¹¹If a user’s device is quarantined, they are going to want to know why, and what to do about it. It has been reported that an ISP can spend 1-2% of all their income on this type of support Steven Hofmeyr and others, “Modeling internet-scale policies for cleaning up malware” [2011] *Economics of Information Security and Privacy III* 149 .

¹¹²Lichtman and Posner (n 40).

¹¹³Anderson and others, “Security economics and european policy” (n 67) at p28.

¹¹⁴ibid.

¹¹⁵Some providers will have a business model of deliberately turning a blind eye, or providing “bullet-proof hosting” services. These services are considered as part of the criminal operations rather than simply being negligent

¹¹⁶The same arguments apply for social media sites and search engines

¹¹⁷Van Eeten and others (n 6).

¹¹⁸See discussion on 7(n 42)

utility of economic efficiency arguments as well, since they will not have deep pockets, or an ability to spread the losses.

This situation is different to an employer/employee relationship though, because the actual control an intermediary could exert is limited. An employee who is negligent on a regular basis, costing his employer money, would not be retained by the company. In this case however, the only option an intermediary might have is to increase the fees for the user, or refuse to serve them at all. Although an ISP may be able to tell which network was participating in DDoS attacks, it would not be a trivial task to determine which machine on the network was. If someone not paying the subscription fee moved to a different network, how would they be able to tell that the risk had materially altered at both places? Refusing to serve someone on account of their risk reduces the value of the Internet for everyone: the account holder doesn't get access to the benefits of the Internet, and for businesses, there are fewer people to interact and spend money on products advertised on the Internet.

In practice, it is unlikely that any liability would fall on one particular group. Insurance companies are good at shifting liability between blameworthy parties, and there are arguments in favour of liability for any of the groups discussed. However, used purely with economics does not appear to offer sufficient justification for a liability model. This is not to preclude the imposition of liability altogether: there are situations where someone has suffered loss and liability is an appropriate means for them to get it back. The victim of the DDoS attack in our scenario (Diane) could claim for losses suffered against any one of the operators of the open recursive resolvers. They are identifiable, and can split liability between themselves, or with the networks allowing source IP address spoofing. The reason this works, is because there is an identifiable victim, and in many cases a quantifiable loss¹¹⁹.

4 Limitations of the Liability Model

So far, analysis has centred on the notions of reducing the incidence of insecurity but this is not the only consideration. The final consideration of the three described by Calabresi is whether the liability regime would actually save any more than it costs¹²⁰. The analysis of the costs of cybercrime by Anderson et al. demonstrated that the costs of cybercrime per person in the country are very small, and the costs industry bears in attempting to mitigate cybercrime represent a significant percentage of those figures¹²¹. Patching, despite potentially having a significant impact, is in itself a cost in both time and effort¹²².

Article 4A UCC which was briefly mentioned earlier provides a cautionary tale for the

¹¹⁹For example, a gambling site would be able to show how many bets they might expect to receive on a comparable day

¹²⁰G Calabresi, *The cost of accidents: a legal and economic analysis* (Yale University Press 1970).

¹²¹Ross Anderson and others, "Measuring the cost of cybercrime" in *Proceedings (online) of the 11th Workshop on the Economics of Information Security (WEIS), Berlin, Germany* (2012).

¹²²ibid.

consequences of using market forces and liability to ensure adequate security. The law places the burden of a loss on the customer for an unauthorised transaction if the bank was operating pursuant to a security procedure and the bank processed the transfers in good faith¹²³. The security procedure itself has to be “commercially reasonable”¹²⁴ based on the circumstances of the customer and the bank, otherwise the bank would be liable for the loss. The official commentary of the legislation suggests that this protects both the customer and the bank, since the bank should be incentivised to provide a commercially reasonable security procedure¹²⁵ and mutual interest of the bank and the customer will ensure that a commercially reasonable procedure will be agreed upon¹²⁶.

Lawsuits are expensive, to successfully claim damages requires costly forensics, legal fees and no guarantee of victory¹²⁷. There is a necessity for a willing class of victims who are prepared to go through this in order to establish precedents of what standards are expected, and to ensure that there is a sufficient risk of lawsuit to ensure it does function as a deterrent. In many cases, the costs are low to an individual and it is only cumulatively that the costs are worth pursuing¹²⁸. Lichtman and Posner suggest that this could be achieved through a class action device, or through a body such as the FTC bringing a lawsuit on behalf of a group of victims¹²⁹, though such a system does not exist in the UK.

Simply using statutory damages paid to the reporter of incidences of insecurity could provide a better solution as it gets around the additional costs associated with liability. Similarly, incentives could be used instead of threatening with liability. For example, Clayton suggested government support for ISPs to remediate devices at a minimal cost¹³⁰. If a market approach is to be used, then some mark of excellence that could be offered to ISPs to indicate their security. This would have the effect of allowing users who would be prepared to pay extra for security¹³¹ to understand which offer a more secure service, and it would also allow the government to offer support to operators who do that, for example in the form of tax breaks¹³². Given users engage in insecure behaviour for marginal economic reward¹³³, it could be possible for government to subsidise a reduction in their Internet connection provided they can demonstrate that they have taken steps to ensure their own security.

¹²³§4A-202(b) U.C.C.

¹²⁴§4A-202(c) U.C.C.

¹²⁵Official Commentary to Article 4A-203 U.C.C., point 3

¹²⁶ibid. Point 4

¹²⁷This is the criticism of liability in general described earlier, seen in Atiyah, *The Damages Lottery* (n 28).

¹²⁸Lichtman and Posner (n 40), Anderson and others, “Security economics and european policy” (n 67)

¹²⁹Lichtman and Posner (n 40).

¹³⁰Richard Clayton, “Might Governments Clean-up Malware?” [2011] (81) *Communication and Strategies* 87 .

¹³¹Dallas Wood and Brent Rowe, “Assessing Home Internet Users’ Demand for Security: Will They Pay ISPs?” In *10th Workshop on the Economics of Information Security* (2011).

¹³²Using the suggestion in Lichtman and Posner (n 40) except that there is no need to retain the liability element.

¹³³Christin and others (n 80).

5 Concluding Thoughts

In this paper, we have performed a literature review of both liability, its impact and security economics. We attempted to utilise the theories from the literature relating to the industrial world, to analyse the impact of liability on different actors in the Internet security area. There are a significant amount of externalities on the Internet which cause difficulties to all concerned, some of which may be internalised through liability, although there are many problems with doing this. Liability on users does not satisfy the economic arguments, and without doing this then any economic benefits for software vendors, websites or intermediaries do not have such a great impact. In certain situations liability is appropriate where there is an identifiable victim and cost, but as a general method of incentivising secure behaviour it does not appear to be supported because of costs in administrating the system and the practicalities of identifying loss and victims prepared to bring lawsuits.

6 Acknowledgements

We would like to thank the anonymous reviewers for their feedback on an earlier version of this paper. This research was funded by the Research Councils UK Digital Economy Program, Web Science Doctoral Training Centre, EP/G036926/1