Legislative and Regulatory Attempts to Address Cybercrime: The Good, the Bad and the Ugly[*]

Douglas E. Salane & Evan Misshula

Center for Cybercrime Studies
Mathematics & Computer Science Department
John Jay College of Criminal Justice

December 10, 2012

Abstract

The past year has been a watershed year for congressional legislation that attempts to address various types of crime that take advantage of the Internet. Major legislation was proposed to protect copyrighted materials and secure critical infrastructures from cyber attacks. Legislation in both areas ran into significant opposition, particularly from Internet and technical communities. Here we examine these measures. We also examine broad based consumer protections that predate the Internet but play a key role in fostering security in the card payment industry, where online transactions are becoming the norm. In examining legislation in these three different domains, our goal is to characterize measures that work and those that are unworkable in the Internet environment. Often legislation devised to address a particular harm in the Internet either misses the mark, or, even worse, can have unintended and undesirable side effects. On the other hand, laws of general applicability, such as longstanding consumer protections, appear to have led the card payment industry to adopt, not perfect, but relatively effective security measures that contain fraud in a dynamic threat environment.

[*] to appear in Cyber Infrastructure Protection 2012, eds., Tarek N. Saadawi and Louis H. Jordan, Jr., Strategic Studies Institute, United States Army War College.

Introduction

The Internet now connects over 2.1 billion people worldwide. In many nations, it provides the basic infrastructure for information services and systems essential for economic and social well-being. With so much riding on the Internet and the modern information systems it supports, all forms of criminal activity are migrating to this realm. In addition, computer systems that control critical infrastructures such as water systems, electrical grids and payment networks often, either advertently or inadvertently, are accessible from the Internet, raising serious security concerns.[1] As misuse and abuse continue to grow, many believe there must be a greater emphasis on law in order to protect individuals, organizations and interests in an Internet environment that provides fertile ground for criminal activity as well as innovation and development.[2]

Yet crafting effective legislation and regulation for this environment presents considerable challenges. While legal and social systems that foster restraint typically are nation state based, modern information systems are transnational in nature and thus so are the crimes. Anonymity on the Internet makes attribution difficult if not impossible, while the transnational nature of the system severely hinders oversight and enforcement. In a system where communications are highly multiplexed, enforcement and oversight measures often require general surveillance and can infringe on privacy and civil rights. The rapid pace of innovation frequently renders technical security standards mandated by regulators ineffective or irrelevant. Even worse, regulatory measures in this realm can produce costly, unintended side effects while not achieving their intended goals. Finally, many fear that measures to guarantee security and protect critical information systems will detract from an open and free Internet and its ability to spawn new development and innovation. On the other hand, without appropriate security, many fear the same result as Internet users increasingly confine themselves to a small collection of "walled gardens" controlled by a few predominant Internet companies, a type of modern feudal system.[3]

We consider cybercrime to be just the contemporary form of crime and make no attempt to develop a taxonomy such as those presented by Council of Europe (2001)[4] or in Anderson (2012).[5] We simply classify as cybercrime any form of illegal activity that takes advantage of the capabilities offered by Internet based systems or that exploits vulnerabilities in those systems. There is now a well developed body of federal and state legislation that takes aim at various activities frequently associated with cybercrime, for example, the widely used Computer Fraud and Abuse Act as well as other statutes that provide penalties for unauthorized access to digital devices or unauthorized interception of electronic communications.[6] Several authors have noted, however, that since cybercrime includes existing crimes migrating to the Internet as well as novel crimes that take specific advantage of modern information systems, laws of general applicability as well as specific laws aimed at Internet crimes are relevant.[7] In this study, we have found financial service sector consumer protections, which predate the widespread use of the Internet for online commerce, appear to be having a significant positive impact in promoting

security and deterring fraud, while laws and regulation aimed particularly at controlling illicit behavior on the Internet often are ineffective or have unintended and undesirable consequences.

In this work, we restrict out attention to recent legislative and regulatory attempts to address the following types of criminal activity: theft of copyrighted materials, fraud in the card payment industry and cyber-attacks on critical infrastructures. Each area has received considerable attention from Congress, federal regulators and industry-wide regulatory authorities. The three areas will continue to be a major concern for the new Administration and Congress since crimes in each of these areas can have significant economic impacts and pose threats to national security[8]. More specifically, here we examine following: 1) the Digital Millennium Copyright Act (DMCA) and more recent proposals designed to protect copyrighted material in a globally connected world, 2) consumer protections and resulting efforts to control fraud in the card payment industry, and 3) recently proposed federal legislation to protect critical infrastructures and address crime involving the Internet.

Although these are three disparate areas, we believe there are lessons to be learned from regulatory efforts in each area. We point out ways existing or proposed legislation and regulation in each area has fallen short of its goals and has had unintended consequences. We discuss the tremendous political difficulties legislation and regulation face as powerful interest groups are pitted against each other. We examine measures that are proving effective in reducing crime in one area and that might be applicable outside that area and lead to more secure systems. We also discuss measures that have proved extremely contentious in the Internet environment and should probably be avoided. As has been suggested by fraud examiners and many security analysts, there is a need for data regarding all forms of cybercrime.[9] Without such data, rigorous empirical studies of what works in reducing cybercrime are not possible.

As noted, what we have found to appear promising are broad based measures that attempt to protect consumers and force transparency – measures in place prior to the rise Internet. Such measures force developers of information systems to design security into the systems, while those deploying systems must maintain a proactive security presence that consistently responds to new threats. In the United States (U.S.), consumer protections have forced banks and credit card associations to put in place elaborate security infrastructures to address constantly changing risks. Available limited data show that these systems, while not perfect, appear to be containing fraud in an online, globally interconnected world.

What do not appear to be effective, and which create the most contention, are measures that attempt to re-architect the Internet or that violate basic Internet design principles. Such measures frequently ignore the scale of the Internet and are unenforceable. Often reactive legislation focused specifically on redressing a specific harm in the Internet environment fits this bill. Measures that force intermediaries, such as service providers, to play an oversight and enforcement role are of particular concern. Such measures often engender significant opposition since they have the potential to impact many Internet users and are not seen to be in the

intermediary's interest. Legislation to protect critical infrastructures also faces significant political challenges since affected industries see only costs and no economic benefits.

The following is an outline of the paper. We begin with a discussion of legislation and regulation to protect copyrighted materials. We then provide an overview of the card payment industry and discuss the impact of strong consumer protections on security practices in that industry. Finally, we compare two recent legislative attempts to improve security in the face of increasing cyber threats to critical information infrastructures. We end by drawing comparisons among established and proposed regulation and legislation. Overall, we believe this study illustrates a basic principle of security economics: the one who will incur the liability has the most interest in providing the security.

Protecting Copyrighted Materials

Industries that traditionally have been content producers, such as the recording and motion picture industries, have faced enormous challenges as their decades old content distribution channels are being displaced by a wide range of Internet based digital content distribution systems. These include social networks such as YouTube and file sharing systems, many of which have been used for sharing copyrighted materials illegally. As content producing companies transition to digital distribution systems, they can no longer rely on restrictions offered by physical media to protect copyrighted materials. Digital media are easily copied and made widely available, often from web sites outside of U.S. jurisdiction.

According to the industry's own statistics, however, its transition to digital distribution is producing strong revenue growth and new subscribers in world-wide markets.[10] Digital distribution resulted in revenues of $5.2 billion in 2011, up 8% from 2010. The industry now derives about 32% of its revenue from Internet sales and access. The number of users worldwide who subscribe to music services such as iTunes and Google Music grew 65% in just one year to 13.4 million. The industry obviously sees digital distribution as the key to future revenue growth. The main concern is that illegal copying and distribution of its digital content will limit that growth[11]. For some time, it has advocated for enforcement and legislation to limit illegal copying and distribution. Currently, it is fostering partnership with content providers to penalize consumers who download copyrighted materials. We discuss these measures later in this section.

In the late 90s the content producers struggled to find means to protect their investments in a rapidly changing world where media were becoming increasingly easy to copy and the new Internet environment was facilitating sharing. National and international calls for copyright legislation arose to address increasing piracy. In October 1998, President Clinton signed into law the Digital Millennium Copyright Act (DMCA)[12]. To protect copyrighted materials, the Act implemented two international treaties, which were developed by the World International Property Organization, a United Nations agency concerned with the protection of intellectual

property.[13] The purpose of the treaties was to coordinate international copyright laws among treaty signatories and make it easier for the signatories to enforce each other's laws.

The DMCA contains two provisions that are of concern here. First, the DMCA prohibits the development or use of copyright circumvention technology. At the time many content producers planned to protect their materials from illegal copying or distribution by imbedding copyright protection mechanisms in the media. These organizations felt anti-circumvention restrictions would prevent bypassing copy right protection technologies. The second measure, the so-called Safe Harbor Provision, provided protection for a nascent Internet content distribution industry, which would soon take advantage of so-called Web 2.0 technologies that featured widespread uploading of user supplied content to web sites. It also was a concession to service providers and the budding search engine industry both of which feared they would be held liable for involvement in the distribution of illegally distributed copyrighted materials. The DMCA limits liability for service providers offering transitory communications, system caching, storage of information on systems at a user's discretion, and information location tools that allow users to find or retrieve materials.[14] A service like YouTube probably never would have achieved the success it did if a single copyright infringement could result in a court order to take down the entire site.

To protect the rights of copyright holders in this new content distribution environment, the DMCA lays out rules for notice and takedown procedures of the infringing item. Copyright holders can notify the service provider's agent that the site is hosting illegally copied material. If the provider promptly takes down or blocks the material, it is exempt from liability. Provisions also protect the provider from legal action brought by the party who posted the material.

The DMCA was controversial from the start. Many questioned how the anti-circumvention measures would affect the "fair use" provisions of copyright law[15]. Until recently, one could be liable for copyright circumvention simply by using a small portion of a copyrighted piece in a remix that was not intended for commercial purposes and that previously would have been legal under fair use provisions. In fact, the illegality would depend largely on how the material was extracted from the copyrighted piece[16]. Many civil rights and Internet advocacy groups object to the DMCA take down provision because a takedown might not be restricted to proven copyright infringement cases and occurs without judicial review. [17]

The Safe Harbor Provision, however, probably had the greatest impact on copyright holders. First, the provision places the burden of "proper notification" on the copyright holder or its representatives, for example, the Recording Industry Association of American (RIAA)[18] or Motion Picture Association of America (MPAA)[19]. Thus, the copyright holder is now put in the position of trying to police the Internet. RIAA representatives complain that it is impossible to monitor all the places on the Internet[20]. In addition, web sites outside U.S. or WTO treaty jurisdictions are immune from the takedown provisions. Finally, the bill sponsors probably

never anticipated the emergence of so-called "cyber lockers," which are not searchable, but where users can share content.

In summary, content providers missed several trends: 1) embedded copyright protections would be of limited use and would actually impede new distribution channels available to the industry, and 2) the takedown provisions of DMCA were unworkable and would give rise to new industries that would challenge their decades old distribution methods. Finally, the DMCA did nothing to address the growth of illegal sharing using peer-to-peer networking, which would take off about a year after DMCA became law. The industry continues to struggle in a world where users can readily upload content. The recent take down of the site Megaupload illustrates the problem.[21] Allegedly users upload content to share in violation of copyright law. The site derives revenue not through the distribution of illegally copied materials, but by offering banner and targeted ads on a very popular web site.

Early in 2012 both houses of Congress considered similar legislation to address the problem of illegal distribution of copyrighted content from web sites outside U.S. jurisdiction. The House considered the Stop Online Privacy Act (SOPA)[22] while the Senate considered the Protect IP Act (PIPA).[23] The Internet and technical communities overwhelmingly opposed both bills. Given the vociferous opposition, the sponsor of the House bill decided not to bring the bill forward for a committee vote. The Senate bill also ran into strong opposition and never came up for a full Senate vote.

SOPA would have empowered the Attorney General (AG) to seek a court order against the owner of a "foreign infringing web site" that enables or facilitates copy right infringement. Service providers and search engines could be required to block a subscriber's access to the infringing site. The act also would have attempted to block revenue to offending sites. For example, it would have prohibited payments to sites from credit card companies and Internet payment services such as PayPal. In addition, it would have blocked online ad companies from doing business with the site.

The most controversial aspect of both bills was Domain Name System (DNS) redirection, which originally was part of both bills. The sponsor removed it from the final version of SOPA in an effort to gain support for the bill. Under this provision, when users type the name of the offending site, the name would connect the user not to the intended site but to content provided by the AG. The actual redirected site would be managed by the ISP but the text would be provided by the AG. The basic enforcement idea behind this site is that you can't go after the infringing web sites so you try to make the intermediaries, for example, search engines and ISPs the enforcers. Of course the AG does not have the resources to police the Internet for illicit content so the AG would designate agents on its behalf, for example, industry representatives such as the RIAA and MPAA.

The enforcement strategy raises both legal and technical questions. Many feel the bill would undermine the Safe Harbor Provisions of the DMCA. Suppose one copyrighted item appeared on the site in question. Does the provider have to block the entire site? Suppose the site in question provides an index to illegally copyrighted content, but also to much content that is not illegal, as might be the case with a BitTorrent Index site.[24] Access to information leading to the offending site would be blocked along with information leading to a significant amount of non-offending content. Several prominent groups of Internet and network researchers have detailed how redirection undermines the Domain Name System (DNS), a key network protocol that makes the Internet usable. [25,26] They assert that DNS redirection schemes would impede the implementation of a new version of DNS that provides greater security, and possibly lead to the creation of an alternate DNS system, which would create a range of security and administrative problems in the Internet. Finally, there is overwhelming agreement in the technical community that redirection and blocking measure could be easily circumvented.

Fearing uncertain costs and possible disruption of their services, the Internet and technical communities strongly opposed both bills. One of the most vocal opponents in congress was the representative from the district that includes Silicon Valley. Despite numerous attempts by the sponsors to make the legislation palatable, for example, elimination of the highly controversial DNS redirection provisions, opponents were able to muster the support needed to derail the legislation. Nonetheless, besides the recording, motion picture and publishing industries, a wide range of organizations and interest groups supported the legislation, including the National Association of Manufacturers, National League of Cities, National Association of Governors and the American Bankers Association.[27]

Recent proposed legislation aimed at protecting copyrighted materials has been fraught with peril. First it pits established content producers (i.e., the publishing, recording and motion picture industries) against a now politically and economically powerful content distribution industry (i.e., Internet companies) Moreover, these companies excel at using their Internet services to deliver their message and win over public opinion. In enlisting service providers and other intermediaries as enforcers, the legislative and regulatory attempts cited repeatedly ignore both the scale of the Internet and a fundamental design principle: keep the complexity at the edges. Thus, many provisions in this legislation are unenforceable and can negatively impact legitimate users of the Internet. Moreover, the proposals raise considerable concerns over privacy and civil rights as they require surveillance of Internet traffic. Furthermore, often overlooked is the fact that the proposed legislation primarily would affect copyright infringement in the U.S. and Europe, but would do little to curtail copyright violations in developing nations, where the content producing industries expect the greatest growth in revenues.

Payment Card Industry

Payment cards, both credit and debit, are an integral part of the modern economy. Consumers use payment cards in over 50 billion transactions per year, more frequently than

cash.[28] Few retail customers are aware of the complex network and numerous entities involved in processing a credit or debit card transaction. Consumers use these instruments with significant confidence and they are the preferred instruments for online transactions, where a consumer never sees the merchant and has to deal with the fundamental insecurities of cyber space. Consumers generally are confident in using their credit or debit cards in such an environment, largely because in most cases they are for the most part shielded from fraud by a variety of legislation as well as the policies of credit card associations and bank issuers.

Figure 1 shows the complexity of the card payment system.[29] The customer only is aware of the card issuer (the bank) and the merchant; however, a transaction could involve each entity appearing in the shaded boxes. Card associations include companies such as Visa and

The Card Payment Network

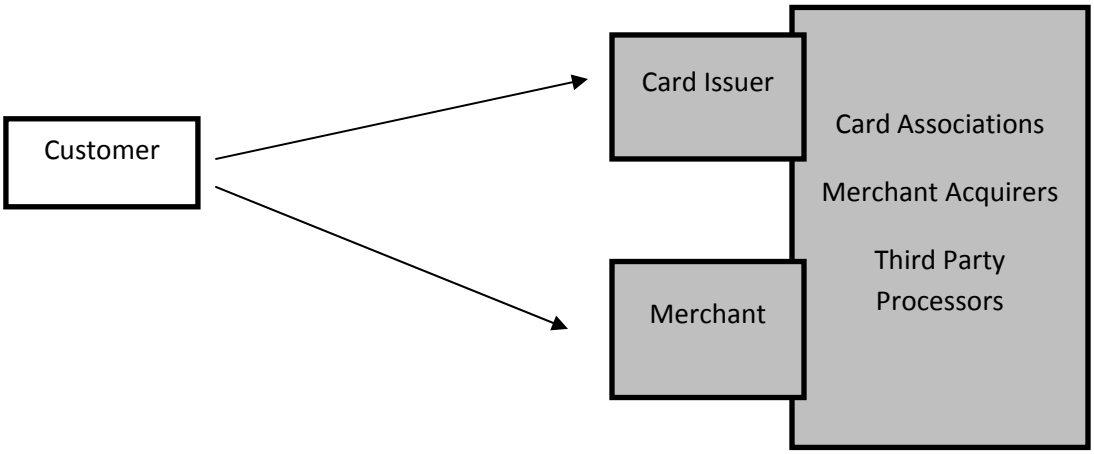

Figure 1

MasterCard, the companies that own the card payment networks and provide the card brands as well as a range of services including fraud monitoring. Merchant acquirers typically are banks that credit merchant accounts when the consumer makes a card purchase. Payment processors,

which include companies like FirstData and Heartland Payment Systems, provide the transaction links between banks, merchants and card associations.

The longstanding regulations that protect consumers in this environment are the Electronic Funds Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z).[30] Regulation Z provides consumer protections for credit card use and accounts for the $50 limit of liability for consumers in fraud cases involving most transactions.[31] Regulation E provides similar if somewhat more limited protection for debit cards. Protection can vary but many debit card issuers in the U.S. now provide noncommercial customers with full fraud protection. There is concern, however, with some newer types of cards such as prepaid debit cards, a small but growing segment of the market, which offer less fraud protection than traditional cards.[32] Consumer advocates widely agree that credit rather than debit cards provide the best fraud protection since a debit transaction results in an immediate charge to a customer's bank account.

The key effect of federal legislation is to keep fraud liability within the gray boxes. Thus, liability is borne by the organizations that offer the services. Contracts and industry-wide regulations, which we discuss shortly, apportion liability among the parties located in the gray boxes. By keeping the liability in the shaded boxes, restricted largely to parties most able to deal with it, the legislation has encouraged industry practices that, although far from perfect, include security at many levels. The industry has been able to manage fraud in an increasingly complex online purchasing world despite massive breaches of card payment information. Fraud on credit card transactions averaged about .15 on every $100 of transactions in the early 90s while today it averages .06 for every $100 of transactions.

Since its inception, fraud has been a key consideration in this industry and early abuses resulted in federal regulations limiting consumer liability if their credit card is used fraudulently. During the past 10 years, however, the industry has faced significant challenges as consumers move to online transactions and its payment system networks become increasingly difficult to secure. Indeed, in recent years the industry has suffered some of the largest recorded data breaches. Data thieves have exfiltrated the card information of hundreds of millions of consumers from retailers, card processors and banks, often by inserting malware on an organization's servers.[33] Although there are glaring security weaknesses, layers of security within each entity in the system do help detect fraud. For example, the massive Heartland data breach in 2009 was discovered not by the card processor but by VISA security, which noticed excessive fraudulent transactions on cards processed by Heartland. In addition, most credit card transactions in the United States go through a real time verification process that is more stringent than in most other countries.

Since 2005, the industry has put in place a set of security standards known as the Payment Card Industry Data Security Standards (PCI-DSS).[34] These are a set of largely technical standards for the security of computers, networks and point-of-sale (POS) equipment, which just about all parties involved in card transactions, must follow. Different standards apply

depending on the number of transactions an organization processes per year. An industry council owned by the card organizations and with representatives from all industry segments oversees the standard and continually updates it to address new risks and technologies.

A data breach can be devastating in this industry. Breaches undermine confidence of both consumers and business partners. Moreover, breach notification and clean up can be extremely expensive – sometimes in excess of $200 per consumer record[35]. Breach notification legislation has played a key role by forcing some transparency[36]. Unfortunately, even within this industry breach details are seldom released in a timely fashion so that if the breach were due to malware endemic in the industry few would know. Yet there is increasing pressure within the industry to share information since confidence of industry partners and consumers depends on transparency.

The regulation PCI-DSS faces numerous criticisms. Few players see it as a strategic initiative and many view it basically as an overhead cost to be weighed against the cost of a breach. [37] PCI-DSS does not address a key industry wide vulnerability – the lack of encryption in the payment network from POS equipment to card issuer. For years a card association has had to ensure the security of its entire payment network. (PCI-DSS only requires encryption if data passes through a public network such as the Internet.) The PCI-DSS standard is variable and places less stringent requirements on smaller vendors and thus fraud may migrate to those vendors. The standard constantly changes and becomes more complex as new threats arise. Thus, compliance becomes increasingly difficult, especially for vendors with limited information technology (IT) resources. Although the standard mirrors the complexity of the systems it is designed to protect, like most standards, it is always behind the curve – threats are dynamic; standards are static. Some consider the PCI standard a form of check box security that diverts IT staff from current threats as they struggle with compliance to avoid legal liability.[38] Finally, merchants often view PCI-DSS simply as a means for card issuers and card organizations to shift liability to them[39]. In the event of a breach, whether the breached party was PCI-DSS complaint or not can play a large role in determining liability.

Compliance with the PCI-DSS standard is difficult to maintain. A 2011 Verizon Business Services study found that only 14% percent of large organizations that were breached were in compliance with the PCI DSS requirement to protect card holder data even though most were compliant at the time of a PCI-DSS audit. In over 100 PCI-DSS audits conducted in 2010, Verizon found that almost 79% of organizations fell out of compliance between audits. [40]

Despite highly publicized breaches of payment card information, the card payment industry has been able to maintain a reasonable security posture in a world where online sales and card not present (CNP) transactions are rapidly becoming the norm. The table in Figure 1 from CyberSource[41] shows the rate of online credit card fraud experience by merchants during the past 12 years. In 2000, merchants lost on average about 3.5% of on-line sales to fraud. After

a considerable drop from 2002 to 2003, we see on-line fraud rates holding steady or trending down. A slight rise in rates occurred from 2010 to 2011.

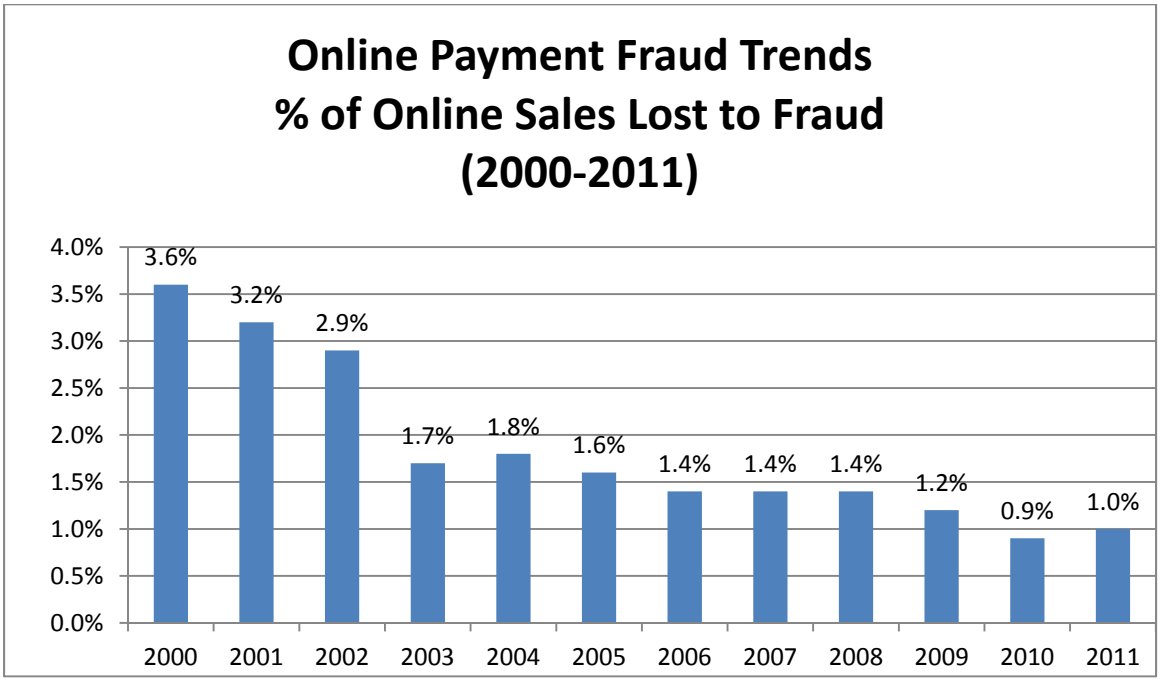

Figure 1

In addition to the CyberSource data, these basic fraud trends are consistent with industry wide data provided by card issuers. Cheney et al[42] note that fraud losses to card issuers have averaged between 5 to 10 cents per $100 of transaction in recent years. The authors note that these losses are only about 10% of the charge-off rate due to credit losses on payment cards.

In a presentation at the Cyber Infrastructure Protection Conference 2012, David Nelson, a fraud examiner with the Cyber-Fraud and Financial Crimes Section of the Federal Deposit Insurance Corporation, found similar fraud trends in card payment industry fraud during the past 6 years[43]. Nelson found absolute losses due to all types of card payment fraud dropped from 2006 to 2007 and then held mostly steady from 2007 to 2011. Nelson's data, mainly from the Treasury Department's Financial Crimes Enforcement Network (FinCen), indicate a slight uptick in fraud from 2010 to 2011[44]. Focusing on level 3 and 4 merchants[45], Nelson noted that the number of payment card fraud reports to FinCen dropped from 2009 to 2011 by over 22%. However, Nelson noted a sharp rise in 2012 bringing the projected number of reports back up to 2009 levels.

One disturbing trend in Nelson's report is a 40% rise in counterfeit card reports last year. Although still a small part of overall card fraud, cybercrime has made vast collections of track 2 data (the data on the card magnetic strip) available to fraudsters. The industry has responded by pushing ahead with the introduction of chip based card technologies (EMV) that deter card counterfeiting.[46] Widespread introduction in the U.S. planned for 2014. With almost universal

adoption of such intelligent card technologies outside the United States, researchers have anticipated rising counterfeit card rates in the U.S. as fraud migrates to nations still using magnetic strip cards.[47] Moreover, limited data indicate that cards issued by non U.S. banks incur higher fraud rates than those issued by U.S. banks when these cards are used in the U.S.[48] Such cards, even though typically chip and pin enabled, maintain the traditional track 2 information on a magnetic strip for compatibility with POS systems in nations that do not employ EMV based equipment. There is considerable pressure from European nations to eliminate magnetic strip entirely and this is a key reason card associations are moving ahead quickly with EMV deployment in the U.S.

It should be noted that the actual fraud losses in the card payment industry are in fact rising since the volume of online sales continues to increase. Yet the CyberSource data show even absolute losses among merchants sampled have been contained to some degree: $3.3 billion in 2009, $2.7 billion in 2010 and $3.4 billion in 2011. CyberSource also reports that the percentage of fraudulent orders has dropped from .9% to .6%, the lowest in 13 years. A vexing problem, however, has been how to lower the rejection rate on international orders, which remains high at 7.3%. The rejection rate represents significant lost opportunity costs when compared with the domestic order rejection rate of only 2.8%.

Of course this data would not inspire confidence if the defense costs needed to keep the rates in check were skyrocketing. According to the CyberSource survey, this is not the case. Costs of fighting fraud as a percentage of sales are the following: .3% in 2009, .2% in 2010 and .1% in 2011. As the total volume of online sales increases, however, the amount spent on defense does rise. Currently it's about double the cost of what was spent five years ago. Despite highly publicized data breaches, the industry appears to be containing fraud in the on-line world without exorbitant rises in security costs.[49]

Several analysts point to higher fraud rates in the U.S. as evidence of the need for a move to a chip and pin system. Several analysts also note that the U.S. has about 47% of the card fraud but accounts for only about 27% of transaction volume world-wide. Certainly, as Europe moves to a mostly chip and pin enabled system, which deters use of counterfeit and stolen cards, analysts expect fraud to increase in CNP payments and in countries still using magnetic strip cards. Others point to a rise in card fraud data which is contrary to the sources cited here. Unfortunately, there is no central source that collects card fraud data for the entire industry and provides a categorical break out. Data is accumulated through voluntary reports so the data must be treated as a sample. More precise reporting of card fraud data is required to fully understand the effects of any regulation and broad abased protections.

Given that fraud rates are higher in the U.S. than Europe, why should anyone think consumer protections have had any positive effect in the US? First, it is difficult to compare U.S. fraud rates with those of European nations. In the U.S., cards are used for a wide range of purchases while in most European countries card use is highly restricted, with cash still playing a

large role in quotidian transactions such as food and restaurant purchases. CNP purchases, which incur higher fraud rates, are lower throughout Europe than in the U.S. In addition, with the U.S. card payment system there is a historical precedent to facilitate the transaction in order to avoid lost sales. Consumers with several credit cards in the wallet will switch to the payment network that is easiest to use. The U.S. system compensates for less secure technology with more extensive online authorization of a transaction than in many card networks outside the U.S. Furthermore, U.S. consumers have learned to protect themselves by using a credit card when making a risky transaction, for example, a CNP transaction where the retailer is not known. Thus, fraud rates are not only the result of security practices but also business considerations, cultural factors and consumer expectations. Our main consideration here has been how the system is holding up in view of the dramatic increase in online transactions. Industry representatives make the case and the data indicate that, despite an uptick in the past year, overall fraud trends in U.S. card payments have remained relatively low and stable[50]. In fact, they only account for about 10% of lost revenue when compared to payment defaults on cards used legitimately.

A recent Federal Reserve Bank report describes how the card payment industry copes as increasingly sophisticated criminals change targets and points of attack and as the number and the types and complexity of payment methods grow.[51] With the umbrella of consumer protections expected to extend to new systems that facilitate credit and debit card purchases, for example, Google Wallet, the card payment industry must take the responsibility for new security threats.[52] Moreover, consumers have become accustomed to the industry providing security and any diminution of that expectation undoubtedly will result in consumer rejection of a new payment system. Several security analysts have noted that in an attempt to lower transaction costs, new payment system providers not subject to existing regulation may attempt to cut costs by skimping on security and shifting liability to consumers. [53]

In summary, long standing regulation, basically consumer protections that limit consumer liability in the event of fraud, have resulted in a card payment system that is able to keep fraud at manageable levels in an environment where rapidly changing technologies continually create new security risks as well as business opportunities. Apportionment of liability among industry players, however, certainly is contentious with PCI-DSS lying at the center of the controversy. Nonetheless, in this arena regulation appears to have resulted in a system which consumers trust and which keeps the industry ever vigilant in the face of changing technologies and risks.

Protecting Critical Infrastructures

Cyber-attacks on computer systems and networks that control critical physical infrastructures or provide essential services have the potential to be the most destructive forms of cybercrime. Recent distributed denial of service (DDOS) attacks on the banking system provide examples of just how disruptive such attacks can be even against organizations with the best

defenses.[54] Besides information systems and financial services, many fear that cyber-attacks could affect critical systems such as water supplies, power grids, treatment plants, chemical facilities and even transit systems. Most of these systems involve computer networks that were once assumed to be private isolated networks. Isolation from the Internet, however, is very difficult to ensure, as the Stuxnet attacks on computers controlling Iranian nuclear facilities clearly illustrated[55]. Moreover, many of these legacy private networks that control critical systems still rely primarily on isolation for security and lack the elaborate layered security controls now typically part of modern interconnected networks and the host devices they support.[56] Finally, many legacy control systems have glaring security vulnerabilities, for example, vendor passwords that have never been changed. Thus, such systems are opportune targets.

Recently, both the House and Senate have considered legislation aimed at protecting cyber infrastructures. The most notable House bill is the Cyber Intelligence Sharing and Protection ACT (CISPA)[57]. The Senate bill that has received the greatest attention is the Revised Cyber Security Act of 2012 (CSA 2012)[58]. The Senate bill has gone through several revisions with the latest version introduced on July 19, 2012.[59] The House bill, commonly known by its acronym CISPA, was approved by the House on April 26, 2012. The Senate bill, after rancorous debate, failed to pass cloture in the Senate on August 2, 2012. The House bill is opposed by the Administration and has not yet been considered by the Senate.

The two bills represent the opposite ends of the spectrum when it comes to addressing the cybercrime question and protecting the nation's critical infrastructures from cyber-attacks. The House bill relies on voluntary information sharing on the part of private industry, particularly Internet companies and Internet service providers. This relatively brief bill, 27 pages, creates no new enforcement structures or regulatory authority. The Senate bill, 212 pages, takes a far more proactive approach. It creates a new government entity responsible for organizing efforts in the private sector to identify critical private sector owned infrastructures vulnerable to cyber-attacks. The bill provides incentives for the private sector to come up with industry-wide plans to protect those infrastructures.

The House bill promotes information sharing by limiting the liability of those who share information with the federal authorities or other private sector entities involved in an effort to contain or thwart a cyber-incident. The key idea is that cyber threat information, as determined by the "covered entities" specified in the bill, should be shared both with government and others affected by the threat. The bill provides little guidance as to what constitutes cyber threat information and few restrictions on what types of information may not be shared. In terms of personally identifiable information (PII), the bill excludes both educational and medical records. Interestingly, the bill contains language that exempts covered entities from liability if they possess cyber threat information and choose not to share it. The bill does not prohibit information gathered to protect national security from being used for other purposes, for example, routine law enforcement.

There was significant opposition to the bill. Due to the lack of limits as to what constitutes cyber threat information and who determines it, privacy and civil right groups adamantly opposed the House bill.[60] The Association for Computing Machinery (ACM), a leading professional computing organization, also opposed the bill, not only on privacy grounds, but also because the bill could result in a "deluge of useless information" that would overwhelm government analysts[61]. Some are critical of the bill's approach since the idea of purely voluntary information sharing has proved thus far to be ineffective in bolstering security. The bill passed the House largely along party lines in April 2012.

The House bill enjoyed fairly broad support in the private sector, especially among companies who own critical infrastructures, offer services on the Internet or provide financial services. For example, the bill received overwhelming support from associations representing the financial services industry including the American Bankers Association,[62] the Electronic Funds Transfer Association,[63] and the Financial Services Information Sharing and Analysis Center (FS-ISAC).[64] Many Technology and Internet companies also embraced the bill largely for its extensive liability protections, with even Google supporting it despite pressure to take a stance against its lack of safeguards for PII. Many argue that despite criticisms of the bill on privacy grounds, it has to be realized that threats of costly legal action are a key reason organizations choose not to release information regarding a data breach[65]. On the other hand, there are no guarantees that organizations would share cyber-threat information in a timely fashion even with the liability limitations provided in the bill.

Unlike CISPA, the Senate bill CSA 2012 would have established a new federal entity to oversee the protection of critical infrastructures vulnerable to cyber-attack. The bill would setup the National Cyber Security Council, which would include key federal agencies and be chaired by the Department of Homeland Security (DHS), whose responsibility would be to identify industries subject to the greatest risks from a cyber-attack. Critical categories of infrastructure would include only infrastructures where a cyber-attack could cause catastrophic damage such as mass casualties, mass evacuations or large scale economic disruption. Industry led groups who control critical private infrastructures would be provided incentives to develop voluntary plans and practices for mitigating risks within the industry. Identified sectors would have to have plans approved by the Council. Once a sector submitted plans, the Council could decide to make the plans mandatory for the sector. Participation would be incentivized through limits of liability to those in compliance with Council adopted practices in the event of a cyber-attack. The bill would provide a framework for sharing information within industries and with federal government while at the same, according to proponents, protecting privacy and civil rights. In addition, the bill contains provisions to strengthen the federal government's networks, improve the federal cyber security workforce and provide for a cyber-security research and development program.

The bill sponsors took precautions to avoid the mistakes of other congressional legislation to regulate activities on the Internet such as recent controversial bills to protect

copyrighted materials on the Internet. The bill does not attempt to regulate networks or individuals by, for example, requiring ISPs to filter traffic. Also, the sponsors tried to ease the concerns of privacy and civil libertarians who feared the bill would abrogate existing privacy and civil right protections. In a stark departure from CISPA, the Senate the bill contains language prohibiting federal authorities from compelling the disclosure of information from a private entity unless otherwise authorized by law or from intercepting a wire, oral, or electronic communication outside the scope of current legal restrictions.[66] Both the ACLU and EFF applauded the inclusion of such restrictions in the bill. The EFF, however, still was wary of a bill that despite protections could further diminish privacy and for which it was not convinced there was a need. Both organizations ultimately opposed the bill.

Economic and partisan interests were the main factors determining support or opposition to the bill[67]. Despite the efforts of the framers toward accommodation for the industries impacted, the bill had significant opposition. As expected many of the industries that own critical infrastructures were reluctant to give the Federal government any new regulatory powers despite the bill's efforts at industry involvement. Even consumer and manufacturing groups opposed the bill fearing a new regime of regulation that would result in new costs. Organizations opposing the bill included American Fuel and Petrochemical Manufacturers, National Association of Manufacturers, Chamber of Commerce, American Public Power Association, Electricity Consumers Resource Council and the National Telecommunications Cooperative Association.

There was a considerable effort to derail final version of the bill in the Senate. Despite its bipartisan sponsorship, it was widely opposed by Republicans. Last minute spurious amendments opponents tried to attach to the bill included the repeal of Affordable Care Act and restrictions on abortions in the District of Columbia. The bill was unable to attract the 60 votes needed for cloture. Although many had reservations about CSA 2012, the bill took the important first step of identifying those physical infrastructures where a cyber attack could cause severe disruptions and losses, a widespread concern that must be addressed.

The list of organizations supporting CSA2012 was not surprising either. The bill certainly had support of many in the software industry, defense industry, computer and network equipment manufacturers and organizations representing schools and colleges. Those charged with protecting the nation from cyber attacks were particularly supportive of CSA2012. For instance, the bill had the strong support of General Keith Alexander, head of the National Security Agency's (NSA) U.S. Cyber Command, who has testified that cyber attacks in the U.S. have increased 18 fold from 2009 to 2011.[68] The bill also had the strong support of the Administration and the Secretary of Defense, Leon Panetta, who lamented a failed attempt to revive the bill in November 2012.[69]

Developing legislating and regulation to protect critical infrastructures is a very tricky business. A recent examination of the resilience of the Internet sponsored by the European

Network and Information Security agency points out some of the difficulties that arise in improving the security of the Internet[70]. Most notable is the "Tragedy of Commons" phenomena. No single network operator is going increase its costs in order to contribute to the "resilience of the whole."[71] The same applies to protecting critical physical and information infrastructure within given industries that rely on the Internet. No organization will support anything that increases its costs unless there are clear benefits to the organization. In the case of CSA 2012, affected organizations saw only costs. A major cyber-attack, however, might quickly change views. In the case of CISPA it was clear how Internet organizations and service providers would benefit from limits on liability for sharing. However, it was not clear anyone would share information even with liability limits. In any event, Lewis and other analysts assert voluntary information sharing and public-private partnerships are simply not working.[72]

In some cases information sharing does take place when the awareness of mutual benefit is obvious and in fact vital. Hall points to the 2010 China Telecom incident where 15% of Internet traffic was routed through an ISP in Beijing for about 20 minutes. At this point security analysts believe it was simply a misconfigured router that led to the event rather than a deliberate effort to reroute traffic and carry out a man-in-the-middle attack[73]. The incident points out a key weakness of the Internet, a trust based routing protocol that assumes all address information is accurate. As Hall points out, despite the weak protocol, operational structures within the Internet resulted in quick correction of the problem. Thus, not only information sharing but cooperation among the players is the key. Those who operate the Internet tend to cooperate and share information when it's clearly in their interest. An important resource for Tier 1 and Tier 2 ISPs is the North American Network Operators Group, which promotes interchanges between major service providers so the Internet runs reliably and securely.[74]

Lessons Learned

This work has provided a brief overview of legislation aimed at protecting intellectual property, card payments and critical infrastructures vulnerable to cyber-attacks**.** The new administration and Congress will receive increasing pressure to provide protections in each of these areas. It is essential that we learn from experience what works and avoid measures that are ineffective, impose additional costs or interfere with the normal functioning of Internet and offer little or no security benefit. Although we examined three disparate areas, each provides examples of the types of measures that appear to achieve the desired results and those that don't.

Strong consumer protections and the need to maintain consumer confidence appear to be the driving forces behind relatively effective security in the card payment industry. Although the system is by no means perfect, the card payment industry does restrict fraud to manageable levels and consistently adapts security infrastructures to address new threats. Yet even in the card payment industry, where liability is restricted to industry players and apportioned through contractual arrangements, few details concerning the nature of attacks have been released during major data breaches of payment processors and others. Nonetheless, in the card payment

industry and credit industry considerable sharing of fraud information does take place through the card associations and third party consultants since fraud impacts these organizations' bottom lines. An example noted earlier was the detection of the Heartland data breach by VISA.

Measures for protecting copyrighted materials have failed because they attempt to make intermediaries the enforcers, and ignore the scale and nature of the Internet. Recent measures in this category are aimed at stopping piracy on web sites outside of U.S. or WTO treaty jurisdictions. Content filtering and DNS redirection do not work since new web sites with illegally copyrighted material can be established far more quickly than anyone can detect and block them. In addition, DNS redirection and content filtering pose both privacy and ethical problems. Too often the industry has tried to accomplish through technical measures what needs to be accomplished through international law enforcement cooperation and international agreements. The sponsors of the CSA 2012 bill wisely avoided filtering requirements while the sponsor of the House bill removed DNS redirection after significant opposition from the Internet and technical communities. Besides being highly contentious, measures such as content filtering and DNS redirection, which require deep packet inspection by intermediaries within the Internet, are contrary to basic Internet design principles.

The legislation we examined to secure critical infrastructures uses a carrot and stick approach, with emphasis largely on the carrot. Under CSA 2012, industries compliant with industry wide security standards would be exempted from liability in the event of a cyber-attack on these infrastructures. CISPA exempts ISPs and other Internet companies from liability for sharing information needed to investigate a cyber-event – and also for not sharing information. In the card payment industry, it is precisely a liability threat that provides incentives for the industry to maintain a significant security infrastructure that must adapt to new risks. There is no evidence that exempting organizations from liabilities promotes information sharing or forces them to provide better security. If organizations who own critical infrastructures are held responsible for collateral damage precipitated by cyber attacks on their critical infrastructures, there would be a strong incentive to take measures to prevent such events.

Legislation or regulation that attempts to mandate technical security standards can present a range of problems. Certainly, industry wide standards are warranted since as the forensic investigations by Verizon and others repeatedly demonstrate, it's the common lapses that hackers often exploit, for example, weak passwords, unpatched software or unnecessary services running on machines. Yet, unlike mandated standards in other domains, for example, building codes, static standards in a dynamic threat environment can often miss the mark. Moreover, as experience with PCI-DSS has shown, mandated standards linked to liability limitations often lead to a system of check box security where resources are shifted toward compliance to avoid liability, which leaves fewer resources available to mitigate emerging threats. In the case of CSA 2012 infrastructure protection bill, the sponsors wisely decided to let the industry develop and approve standards while the Council would oversee the adequacy of

those standards. The sponsors, however, may have overlooked the difficulty of establishing and maintaining effective security standards in a dynamic threat environment.

In each area examined, industry lobbies rally to protect sector interests, which means any legislation faces difficult hurdles in Congress. Compromises that must be built into legislation to get it passed frequently water it down to a point where it cannot be effective. As one of the sponsors of CSA 2012 recently indicated, however, a key point in the bill that remained was the requirement that organizations report cyber-attacks on systems controlling critical infrastructures.[75] Without such a record, it is impossible for defense and security analysts to know the exact nature or frequency of attacks and take defensive measures. As many have pointed out, it should not take a kinetic incident to make us aware that cyber-attacks on systems controlling critical infrastructures are taking place.

Finally, a point often overlooked is that the Internet is a collection of networks that must be managed by cooperating players. If a major player such as a nation state attempts to undermine the system, for example, by inserting inaccurate routing or DNS information, all bets are off. The Internet as we have known it simply will no longer exist.

Concluding Remarks

Here is a brief summary of what we consider the good, the bad and the ugly encountered in this study. The good includes legislation that protects consumers and limits liabilities to those who offer the systems and are able and obligated to contain the risks for all parties. The bad includes legislation that forces intermediaries such as ISPs or other third party organizations to provide oversight and enforcement in ways that don't scale on the Internet or that disrupt the normal functioning of the Internet. The ugly is the ideological and partisan bickering that prevents serious discussion of measures needed to protect critical information and physical infrastructures from cyber-attacks.

End Notes

[1] E. Bumiller and T. Shanker, "Panetta Warns of Dire Threat of Cyberattack on US," *New York Times*, October 11, 2012.

[2] F. Cate, "Security, Privacy, and the Role of Law," *IEEE Security and Privacy*, Vol. 7, No. 5, January 2009, pp. 60-63.

[3] J. Zittrain, *The Future of the Internet and How to Stop It*, New Haven and London: Yale University Press, 2008.

[4] Council of Europe, "Convention on Cybercrime," CETS No.:185, Budapest, November 2001, available from conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[5] R. Anderson, C. Barton, R. Bohme, R., Clayton, R., van Eeten, M.J.G, Levi, M., Moore, T. and Savage, S "Measuring the Cost of Cybercrime," *11th Annual Workshop on the Economics of Information Security (WEIS 2012)*, WEIS, Berlin, Germany, June 25-26, 2012.

[6] M.M. Losavio, J.E. Shutt and D.W. Keeling, "The Information Polity: Social and Legal Frameworks for Critical Cyber Infrastructure Protection," in T. Saadawi and L. Jordan, Jr., eds., *Cyber Infrastructure Protection*, Strategic Studies Institute, U.S. Army War College, May 2011, pp. 129-154.

[7] S. K. Mehra, "Cybercrime in the United States Today," *American Journal of Comparative Law*, Vol.58, 2010, pp. 659-686.

[8] S. Sengupta and E. Wyatt, "The Internet Remains a Tangle of Issues," *New York Times*, November 8, 2012.

[9] Anderson et al, "Measuring the Costs of Cybercrime."

[10] International Federation of the Phonographic Industry, "IFIP Digital Music Report 2012 : Key Facts and Figures," available from www.ifpi.org/content/library/DMR2012_key_facts_and_figures.pdf, accessed October 1, 2012.

[11] Ibid, p. 2.

[12] U.S. Copyright Offices Summary, "The Digital Millennium Copyright Act of 1998,"available from www.copyright.gov/legislation/dmca.pdf, accessed August 2, 2012.

[13] World Intellectual Property Organization, available from www.wipo.int/about-wipo/en/, accessed September 2, 2012.

[14] U.S. Copyright Offices Summary, "The Digital Millennium Copyright Act of 1998," Title II, p. 8.

[15] P. Samuelson, "Why Anti-circumvention Regulations Need Revision," *Communications of the ACM*, Vol. 42, No. 9, September 1999, pp. 17-21.

[16] R. Tushet, "Law and Technology: Remix Nation," *Communications of the ACM*, Vol. 54, No. 8, September 2011, pp. 21-24.

[17] Electronic Frontier Foundation, "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands," September 25, 2003, available from www.eff.org/wp/unsafe-harbors-abusive-dmca-subpoenas-and-takedown-demands.

[18] www.riaa.com

[19] www.mpaa.org

[20]D. McCullagh, "RIAA: U.S. Copyright Law Isn't Working," CNET, August 23, 2010, available from news.cnet.com/8301-13578_3-20014468-38.html, accessed October 1, 2012.

[21] M.J. Schwartz, "Megaupload Takedown Questioned by Uses, Lawyers," *Information Week*, January 23, 2012, available from www.informationweek.com/security/client/megaupload-takedown-questioned-by-users/232500305, accessed September 10, 2012.

[22] Stop Online Privacy Act, H.R. 3621, 112th Congress, 1st Session, 2012, available from www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf.

[23] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Congress, 1st Session, available from www.govtrack.us/congress/bills/112/s968/text.

[24] Wikipedia, "BitTorrent," available from en.wikipedia.org/wiki/BitTorrent, accessed November 1, 2012.

[25] S. Crocker, D. Dagon, D. Kaminsky, D. McPherson, P. Vixie, "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the Protect IP Bill," white paper, May 2011, available from www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf, accessed August 30, 2012.

[26] Sandia National Laboratories, letter to the Honorable Zoe Lofgren, member of Congress, technical assessment of DNS filtering provisions of SOPA and PIPA, November 16, 2011, available from www.scribd.com/doc/73106069/Napolitano-Response-Rep-Lofgren-11-16-11-c, accessed September 1, 2012.

[27] www.scribd.com/doc/76607770/Updated-SOPA-Supporters

[28]Presentation by C. Merritt, Retail Payment Risks Forum, available from www.nacha.org/userfiles/File/USIC/FFIEC%20Fraud%20Forum%20cmerritt%202010%20%282%29.pdf, accessed September 1, 2012

[29] R. P. DeGennaro, "Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box," *Economic Review - The Federal Reserve Bank of Atlanta*, v. 91, no. 1, 2006, pp. 27-42.

[30] The most recent versions of these regulations are provided by the Board of Governors of the Federal Reserve System on its Regulations web page, available from www.federalreserve.gov/bankinforeg/reglisting.htm, accessed November 2, 2012.

[31] FDIC Law, Regulations and Related Acts, Part 226 Truth in Lending (Regulation Z), available from www.fdic.gov/regulations/laws/rules/6500-1400.html.

[32] National Consumer Law Center, Comments to the Federal Trade Commission, August 28, 2012, available from www.nclc.org/images/pdf/banking_and_payment_systems/mobile-comments-by-nclc-to-ftc-28-aug-2012.pdf.

[33] D.E. Salane, "Are Large Scale Data Breach Inevitable," *Cyber Infrastructure Protection*, eds. T. Saadawi and L. Jordan, Strategic Studies Institute, U.S. Army War College, Carlisle, PA,. 2011.

[34]PCI Security Council, "PCI –DSS," available from www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0, accessed August 30, 2012.

[35] Poneman Institute, "2011 Cost of a Data Breach Study," March 2011, available from www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-cost-of-a-data-breach-2011, accessed September 1, 2012.

[36] Payment systems such as Google Wallet that allow users to store credit cards in a cell phone and make payments simply by putting the cell phone near a device in the store typically are covered by both legislated liability restrictions and fraud liability policies of most card networks.

[37] Poneman Institute, "2009 PCI-DSS Compliance Survey," September 24, 2009, available from www.impervia .com, accessed June 1, 2012

[38] Ibid.

[39] J.S. Cheney, R.M. Hunt, K.R. Jacob, R.D. Porter and Bruce J. Summers, "The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risk Posed by Data Breaches," Federal Reserve Banks of Philadelphia and Chicago, October 2012, Philadelphia, PA, available from www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2012/D-2012-Efficiency-and-Integrity-of-Payment-Card-Systems.pdf, accessed November 1, 2012.

[40]Verizon, "Verizon 2011 Card Industry Compliance Report," available from www.verizonbusiness.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf, accessed August 30, 2011.

[41] CyberSource, "2012 Online Fraud Report," available at www.cybersource.com, retrived Sept. 1, 2012. CyberSource is a Visa company that provides fraud detection products for retail merchants. The fraud losses were compiled from surveys of 383 merchants representing a total of $83 billion in online sales in 2011.

[42] www.nilsonreport.com/pdf/news/112111.pdf

[43] D.M.Nelson, "Cyber Crime The Musical," presentation at Cyber Infrastructure Protection Conference, sponsored by the City College of New York and the U.S. Army War College Strategic Studies Institute, New York, NY, September 13-14, 2012.

[44] The Financial Crimes Enforcement Network (FinCen), www.fincen.go, accessed September 10, 2012.

[45] Type 3 and 4 merchants are classifications used by the PCI Council to describe merchants and are based on yearly transaction volumes. Type 3 and 4 merchants typically are smaller businesses that process under 1 million card transactions per year. They also are the most vulnerable to fraud since they and

their acquirers are less likely to have in place the sophisticated fraud detection systems employed by larger enterprises.

[46] Chip based card technologies are based on the Europay MasterCard and Visa(EMV) standards developed in the 90s. A microprocessor embedded in the card or mobile phone is capable of cryptographic processing providing for more robust authentication, for example, ensuring the card holder is authorized to use the card. See www.emvo.com for details.

[47] D. King, "Chip-and-Pin: Success and Challenges in Reducing Fraud," Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January 2012, available from http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf.

[48] R.J. Sullivan, "The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy," presented at the 2010 Workshop of the Economics of Information Security, Harvard University, May 2010, Table 4, p.11, available from www.kansascityfed.org/Publicat/EconRev/PDF/10q2Sullivan.pdf.

[49]Large scale data breaches of track II card information typically result in relatively few cases of identity fraud.

[50] Interview with Eduardo Perez, head of Global Payment System Security for Visa Inc., available at www.bankinfosecurity.com/answer-to-card-fraud-a-3419/op-1, accessed August 30, 2012.

[51] J.S. Cheney, R.M. Hunt, K.R. Jacob, R.D. Porter and Bruce J. Summers, "The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risk Posed by Data Breaches," October 2012, available from www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2012/D-2012-Efficiency-and-Integrity-of-Payment-Card-Systems.pdf, accessed November 15, 2012.

[52] M. Crowe, M. Kepler and C. Merritt, "The US Regulatory Landscape for Mobile Payments," Summary report of the Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators on April 24, 2012, issued by the Federal Reserve Banks of Atlanta and Boston, July 25, 2012, available from www.frbatlanta.org/documents/rprf/rprf_pubs/120730_wp.pdf, accessed on October 3, 2012.

[53] R. Anderson, "Risk and Privacy Implications of Consumer Payment Innovation," paper presented at the conference Consumer Payment Innovation in the Connected Age, Federal Reserve Bank of Kansas City, Kansas City, Mo, March 29-30, 2012.

[54] C. Strom and E.Engleman, "Cyber Attacks on U.S. Banks Expose Computer Vulnerability," Bloomberg News, September 28, 2012, available from www.bloomberg.com/news/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html.

[55] G. Gates, "How a Secret Cyber Program Worked," New York Times Interactive, available from www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?pagewanted=all, accessed on October 30, 2012.

[56] J. Backfield and J. Bambenek, "Network Security Model," *SANs Institute: InfoSec Reading Room*, SANS Institute, 2008, available from www.sans.org/reading_room/whitepapers/modeling/network-security-model_32843.

[57] Cyber Intelligence Sharing and Protection Act, H.R.3523, 112th Congress, 2nd Session, 2012, available from ww.gpo.gov/fdsys/pkg/BILLS-112hr3523eh/pdf/BILLS-112hr3523eh.pdf.

[58] Cyber Security Act of 2012, S. 3414, 112th Congress, 2nd Session, 2012, available from www.gpo.gov/fdsys/pkg/BILLS-112s3414pcs/pdf/BILLS-112s3414pcs.pdf.

[59] A prior version of the bill entitled Protecting Cyberspace as a National Asset was introduced in the Senate in 2010.

[60] R. Reitman, "EFF Condemns CISPA, Vows to Take Fight to the Senate," Electronic Frontier Foundation, available from www.eff.org/deeplinks/2012/04/eff-condemns-cispa-vows-take-fight-senate, accessed June 1, 2012.

[61] E.H. Spafford, comments on Cyber Intelligence Sharing and Protection Act, U.S. Public Policy Council of the ACM, June 6, 2012, available from usacm.acm.org/images/documents/USACMCISPAStatement.pdf.

[62] American Bankers Association, www.aba.com/Pages/default.aspx, retrieved September 1, 2012.

[63] Electronic Funds Transfer Association, letter to house leaders supporting H.R. 3523, available from www.efta.org/files/pdf/efta_issue_454.pdf.

[64]Financial Services Information Sharing and Analysis Center (FS-ISAC),www.fsisac.com/about/, accessed on September 1, 2012. A 1998 presidential directive lead to the establishment of FS-ISAC by the financial service sector to share information about physical and cyber security threats.

[65] R. Dodge and Greg Shannon, "Cyber Security CPR: Coordinated Responses to Cyber Security Incidents," Summary of a workshop sponsored by the Institute for Information Infrastructure Protection, the Software Engineering Institute Computer Emergency Response Team (SEI-CERT), Arlington, VA, October 12-13, 2011, available from www.thei3p.org/docs/publications/451.pdf.

[66] Cyber Security Act of 2012, S. 3414, 112th Congress, 2nd Session, 2012, Sec. 244, Prohibited Conduct.

[67] Open Congress, "S.3414-CSA2012," available from www.opencongress.org/bill/112-s3414/money, accessed on October 30, 2012.

[68] Wilson Center, "Cyber Gridlock: Why the Public Should Care," available at www.wilsoncenter.org/event/cyber-how-to-bring-informed-public-the-debate, accessed October 20, 2012.

[69] Department of Defense, *American Forces Press Service*, "Panetta 'Disappointed' as Cyber Legislation Stalls," available from www.defense.gov/news/newsarticle.aspx?id=118546, accessed November 16, 2012.

[70] C. Hall, C., R. Clayton, R. Anderson, and E. Ouzounis, *Inter X: Resillience of the Internet Interconnection Ecosystem*, European Network and Information Security (ENISA), European Union, April 2011.

[71] Ibid. p.23

[72] James Lewis, Director, Center for Strategic and International Studies, Technology and Public Policy, "What is the Best Way to Protect U.S. Critical Infrastructure from Cyber-Attack," Interview with Scientific American, February 2011.

[73] Renesys Blog, "China's 18 Minute Mystery," available from www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml, accessed January 15, 2011.

[74] North American Operators Group, www.nanog.org, accessed July 1, 2012.

[75] Wilson Center, "Cyber Gridlock: Why the Public Should Care," comments by Senator Susan Collins.