STATEMENT

of

Paul Rosenzweig
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Visiting Fellow, The Heritage Foundation
Washington, D.C.

before the

Committee on the Judiciary
United States Senate

March 13, 2012

Cybersecurity Information Sharing and the Freedom of Information Act

Introduction

Chairman Leahy, Ranking Member Grassley, and Members of the Committee, I thank you for your invitation to appear today and present testimony on the question of cybersecurity information sharing and the Freedom of Information Act (FOIA). My name is Paul Rosenzweig and I am the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice. I am also a Senior Advisor to The Chertoff Group and a Professorial Lecturer in Law at George Washington University where I teach a course on Cybersecurity Law and Policy. In addition, I serve as a Visiting Fellow with a joint appointment in the Center for Legal and Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.[1] From 2005 to 2009 I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

[1] The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2010, it had 710,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2010 income came from the following sources:

Individuals	78%
Foundations	17%
Corporations	5%

Needless to say, my testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Much of my testimony today is derived from prior academic work I have done in this field, most notably a research paper I published under the auspices of the Hoover Institution's Koret-Taube Task Force on National Security and Law, entitled "Cybersecurity and Public Goods: The Public/Private 'Partnership.'"[2] The paper, in turn, will appear as two chapters in my forthcoming book, *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World* (Praeger Press 2012).

In my testimony today, I want to make six basic points:

- The cyber threat is real and likely enduring;
- The sharing of cyber threat and vulnerability information is a classic public good whose creation needs to be enabled by the government;
- Current law is, at best, ambiguous (and at worst prohibitory) and therefore impedes the creation and sharing of cyber threat and vulnerability information;
- The legal régime therefore requires modification to authorize and enable the sharing of vital cyber threat and vulnerability information;
- Essential sharing by the private sector will not occur if ambiguity is maintained or the specter of disclosure is not relieved; and
- Finally, it is therefore essential that a blanket FOIA exemption be part of any new cybersecurity information-sharing legislation.

The Cyber Threat Is Real

On the day I sat down to begin drafting this testimony the NASA Inspector General reported that a significant Chinese penetration of the computer system at the Jet Propulsion Laboratory had occurred.[3] Something on the order of 22 gigabytes of data that contained export-restricted information had been exfiltrated from the computer system of one of the most prominent American laboratories over a period of several months. Sensitive U.S. space information was stolen or destroyed and a laptop with the algorithms to control the International Space Station was also stolen. Only recently had all of this come to light.

The top five corporate givers provided The Heritage Foundation with 2% of its 2010 income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

[2] http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf

[3] http://quantum.nasa.gov/materials/2012-01-21-A4-Williams.pdf

This is not, of course, the only recent evidence of cyber vulnerability. Consider the recently analyzed GhostNet malware.[4] That malware imported a Trojan horse program onto infected computers which allowed a remote user to, effectively, control the computer. The remote user could activate a keystroke logger, turn on the computer's video camera or microphone, and, of course, exfiltrate any data stored on the computer. First observed on computers operated by the Dalai Lama, the malware was found in dozens of other computers including some located in the embassies of India, Malaysia and Indonesia, ministries of foreign affairs, and even NATO (SHAPE) headquarters (albeit on an unclassified system). Extended analysis eventually traced the malware to an IP address on Hainan Island off the coast of China, an island that, perhaps coincidentally, is home to the headquarters of China's signals intelligence agency.

More prosaically, we know that cyber crime is epidemic and growing. Concrete estimates of the economic costs of cyber crime and cyber intrusions are available and offer some indication of the scope of the problem but are, in some views, highly conjectural. For example, the consulting firm Detica has estimated the annual loss from cyber intrusions in the United Kingdom at £27 billion.[5] Two years earlier, McAfee Security estimated the annual cybercrime losses at $1 trillion globally.[6]

These estimates may well be inflated by their methodology. The lion's share of these losses are estimated to flow from the theft of intellectual property (i.e., some form of industrial espionage) with actual monetary loss estimates running roughly an order of magnitude less (i.e., £3.7 billion annually in the UK from fraud and identity theft).[7] If the same factor were applied to the McAfee global number then the annualized monetary loss worldwide would be $100 billion – a significant number but by no means astronomical. More notably, this data is a rough estimate at best – and they produce figures that are inherently suspect. [Full disclosure: At least one critic, for example, has characterized the Detica study as "nonsense" and "a grubby little piece of puffery."][8]

Perhaps somewhat more authoritatively, the Government Accountability Office, repeating an estimate made by the Federal Bureau of Investigation (FBI), believes that in 2005 the annual loss due to computer crime was approximately $67.2 billion for U.S. organizations. The estimated losses associated with particular crimes include $49.3 billion in 2006 for identity theft and $1 billion annually due to phishing.[9]

---

[4] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor* (Mar. 29, 2009), http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

[5] "The Cost of Cyber Crime," Detica (Feb. 14, 2011), http://www.detica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf.

[6] Elinor Mills, "Study: Cybercrime costs firms $1 trillion globally," *CNet News* (Jan. 28, 2009), http://news.cnet.com/8301-1009_3-10152246-83.html.

[7] "The Cost of Cyber Crime," *supra*.

[8] "Cost of Cyber Crime is not Science Fiction, Says Detica," *Information Age* (May 4, 2011), http://www.information-age.com/channels/security-and-continuity/company-analysis/1621903/cost-of-cyber-crime-is-not-science-fiction-says-detica.thtml.

[9] GAO, "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," (GAO-07-705, June 2007). These figures are also broadly consistent with the estimate of $140 billion annual losses made by Ferris

One massive study of Internet traffic conducted for Bell Canada demonstrates both the scope of the problem and the difficulty of definitively assessing its severity. The study reviewed 839 petabytes of data,[10] containing over 4 billion emails each month, carrying more than $174 billion (in Canadian dollars) of commerce every day. Within this flood of data, over 53 gigabytes per second (!) contained malicious code of some sort. The investigators observed on the order of 80,000 zero-day exploits per day and estimated that more than 1.5 million compromised computers attempted more than 21 million botnet connections each month.[11] This data is more or less consistent with estimates by large cybersecurity companies: Symantec, for example, discovered 286 million new, unique malicious threats in 2010, or roughly 9 new malware creations every second.[12] And yet, from all this, the most that can be said is that a large number of financial transactions are at risk – data about actual harm remains painfully elusive.

Cyber Threat Information is a Classic Public Good

Defining a Public Good -- A public good is a good that is both nonrivalrous and nonexclusive.[13] In other words, its use by one person does not affect its use by others and its availability to one person means that it is also available to every other person. The classic example of a public good is national defense. The enjoyment of defense services provided to protect one citizen does not affect the protection enjoyed by another citizen, and defense services provided to one citizen are enjoyed by all other citizens. By contrast, private goods (like, say, a shoe) cannot be used by more than one person (at least at the same time!) and their use by one person affects potential uses by others.

Public goods are, typically, beset by two problems – free riders and assurance. Free-rider problems arise when an individual hopes to reap the benefits of a public good but refuses to contribute to its creation because he thinks others will do so even absent his participation. The assurance problem exists when people refuse to invest in the production of a public good because they believe there will never be enough cooperative investment to produce the good and, thus, that the investment would be futile.

Research, as reported in "Cybersecurity: Where is the Security?" (May 12, 2010), http://www.milesstockbridge.com/pdfuploads/640_Miles_Cyberspace_092410.pdf Phishing is the colloquial phrase used to define efforts to trick unwary to voluntarily disclose their identity and passwords.

[10] This is an immense amount of data. It is roughly 1,000,000 gigabytes and the storage capacity to hold that much data must have cost several hundreds of thousands of dollars.

[11] *Combating Robot Networks and Their Controllers* (Unclassified Version 2.0, May 6, 2010), http://www.scribd.com/doc/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0. One of the authors of the report, Rafal Rohozinski, gave a colloquial talk on this study to the St. Galen Symposium earlier this year. *See* http://www.youtube.com/watch?v=DpRYXRNWka0&feature=youtu.be.

[12] Christopher Drew and Verne G. Kopytoff, "Deploying New Tools to Stop the Hackers," *The New York Times*, June 17, 2011, sec. Technology, http://www.nytimes.com/2011/06/18/technology/18security.html.

[13] *See generally* Paul Samuelson, "The Pure Theory of Public Expenditure" *Review of Economics and Statistics,* 36 (4): 387–389 (MIT Press 1954); David Schmidtz, The Limits of Government: An Essay on the Public Goods Argument (Westview Press 1991).

The classic solution to this conundrum is governmental intervention. When a public good is viewed as necessary but cooperation is unavailing, the government coerces its citizens to cooperate through taxation or some other mandate or incentivizes its creation through a subsidy and thus provides the public good.

Cyber Threat and Vulnerability Information as a Public Good -- Security in cyberspace, like physical security in the kinetic world, is a market good. People will pay for it and pay quite a bit. But, as in the real world, security in cyberspace is not a singular good – rather it is a bundle of various goods, some of which operate independently and others of which act only in combination. Broadly speaking, these goods are purchased in an effort to protect networks, hardware, data in transit, and stored data from theft, destruction, disruption, or delay.[14]

Given the breadth of the scope of the concept of cybersecurity goods, it is unsurprising that different aspects of the bundle may be provided by different sources. Just as some security in the physical world can be purchased directly in the private market, so too in cyberspace many security systems (e.g., anti-virus software and intrusion detection systems) are private goods, bought and sold between private sector actors. They are rivalrous (because their use affects other actors) and excludable (since their owner can limit their use by others). Indeed, evidence from the financial sector suggests that cybersecurity is to a very large degree a private good, adequately provided by the private sector.[15]

There is, however, one aspect of the bundle of cybersecurity goods that appears clearly to be a public good – threat and vulnerability information.[16] That sort of information is both non-rivalrous (giving it to one person to use does not affect how another might use it) and it is non-exclusive (everyone can use the information when it is made available). This public good-like nature of information about cyber threats and vulnerabilities helps to explain the substantial focus of many on laws and regulations regarding information sharing – our legal mechanisms haven't adequately captured the nature of the information being shared and are thought to be an impediment to the wide distribution of this public good, rather than enhancing that activity. It also explains, at least partially, why Google might look to NSA for assistance. They seek a public good, namely information about threats to their systems.

And, of course, this insight into the nature of security information is also consistent with a micro-economic understanding of the incentives that attend the willingness of any individual actor to disclose information about threats and vulnerabilities in its system. There are a host of reasons why private

[14] Eric A. Fisher, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Opinions* 7 (Nova Science Publishers 2009).
[15] Benjamin Powell, *Is Cybersecurity a Public Good? Evidence From the Financial Services Industry*, 1 J.L. Econ. & Pol'y 497, 498 (2005).
[16] Bruce H. Kobayashi, "Private Versus Social Incentives in Cybersecurity: Law and Economics," *in The Law and Economics of Cybersecurity* 16 (Mark F. Grady & Francesco Parisi eds., Cambridge University Press 2006). I am assuming, here, that information is a "good." Some have argued that in the absence of artificial intellectual property protections, information is not a traditional economic good. *E.g.* Murray N. Rothbard, *Man, Economy, and State: A Treatise on Economic Principles 1033* (Ludwig von Mises Institute, Scholar's Ed., 2d. ed. 2009).

sector actors may be reluctant to make such disclosures (especially of vulnerabilities), including: risk of loss of reputation and trust; risk of liability and indemnification claims; negative effects on financial markets; signals of weakness to adversaries; and job security and individual career goals.[17] Treating information as a public good tends to overcome these factors.

The Ambiguity in Current Law

This understanding of the economics of cybersecurity suggests why a significant fraction of the policy debate about cybersecurity and public/private partnerships revolves around the challenge of effective security information sharing. It is often said that existing legal restrictions prevent the private sector from effectively creating cybersecurity. Some of these restrictions are said to relate to the inability of the government to adequately share threat information with the private sector. Other restrictions, more relevant to the subject matter of this Hearing, are said to limit how the private sector shares information with the government or amongst itself.[18]

The focus makes sense when seen through the prism of our theoretical model – because threat and vulnerability information may have the characteristics of a public good, it is affirmatively in society's interests to foster their creation and distribution. If existing laws restrain and restrict either of these, that would be a policy dissonance. On closer examination, many of these legal limitations appear to be less constricting than they are perceived to be. In the end what really restricts cooperation are the inherent caution of lawyers who do not wish to push the envelope of legal authority and/or policy and economic factors (of the sort described above) that limit the desire to cooperate.

The information in question will relate, broadly speaking, either to specific threats from external actors (for example, knowledge from an insider that an intrusion is planned) or to specific vulnerabilities (as, for example, the identification of a particular security gap in a particular piece of software). In both situations, the evidence of the threat or vulnerability can come in one of two forms: either non-personalized information related to changes in types of activity on the network, or personalized information about the actions of a specific individual or group of individuals.[19]

---

[17] E. Gal-Or & A. Ghose, "The economic incentives for sharing security information," *Information Systems Research*, 16 (2), 186–208 (2005).

[18] One important caveat is in order at this point: Information sharing is no panacea. It can, and will, help in preventing attacks where the threat signatures are known. It is ineffective, however, in preventing "zero-day" attacks – that is attacks that are effective on the "zeroth day" because nobody knows about them. In many ways, the problem is very much like the problem with preventing disease – and information sharing is like widely distributing a known, effective vaccine. But no amount of information sharing (or vaccination) can protect you against a brand new virus.

[19] Network traffic information can be information relating to suspicious packets, including ports, protocols, and routing information; specific virus/other malware signatures; IP addresses; and the identification of particularly suspect domains or servers. Personally Identifiable Information (PII) includes more person-specific types of information such as, identifying websites accessed; times and locations of logins/account access; discrepancies in user names; or content of communications and is, more typically, related to a specific malfeasant activity (such as an attempted fraud, identify theft or the transfer of terrorist finances).

Private-to-Private and Private-to-Government Sharing -- Consider the laws that are often said to limit the ability of the private sector to cooperate with the government or amongst itself. Two portions of the Electronic Communications Privacy Act (ECPA),[20] Title I, relating to wiretapping (sometimes spoken of as an amendment to the Wiretap Act),[21] and Title II, relating to the privacy of electronic communications (often called the Stored Communications Act (SCA)),[22] are of facial applicability. These laws were created to protect privacy and to impose checks and balances on law enforcement access to private citizens' communications. As such they serve important public policy goals.

But it is equally true that the laws are of old vintage. Passed initially in 1986, they were largely drafted to address issues relating to the telephone network, and, it is fair to say, have yet to be fully modernized to come to grips with today's Internet-based communications technologies. Some Internet service providers argue that the ambiguous nature of the laws and their applicability prevent them from acting to protect the customers and their networks by making it legally uncertain whether or not they can use certain communications information to protect consumers and/or share certain information voluntarily with the government for purposes of cybersecurity.

Accordingly, they argue, some changes are necessary in law to clearly authorize cooperative cyber activities. The SCA, for example, generally prohibits an electronic communications provider or a remote computing services provider from disclosing the contents of electronic communications or information about a customer who subscribes to its services, absent appropriate legal process. Likewise the Wiretap Act prohibits the interception of communications in transit, except according to legal authorization. The general prohibitions are said to inhibit information sharing of cyber-related threat information.

The arguments for ambiguity are, however, somewhat overstated. Both laws have exceptions reasonably related to the protection of service provider networks. The SCA permits information to be divulged "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service."[23] The phrase has rarely been interpreted (and indeed the one notable case interpreting it involved Apple's argument that it authorized compliance with a civil subpoena, since to fail to do so would cause it to lose money).[24] But there is no reason to suppose that the phrase "protection of property" does not encompass protection of the network that the service provider maintains. To be sure, this requires a slight interpretive leap but it is slight enough that it is difficult to understand the legal hesitancy of network providers on this score.

[20] Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848.
[21] Title I is codified at at 18 U.S.C. § 2510 *et seq.* The original Wiretap Act was passed in 1968 as Title III of the Omnibus Crime Control Act.
[22] Title II is codified at 18 U.S.C. § 2701 *et seq.*
[23] 18 U.S.C. §2702(b)(5), (c)(3).
[24] *O'Grady v. Superior Ct.*, 139 Cal.4th 1423 (2006).

Indeed, this "provider protection" language is copied from the provider exception of the Wiretap Act,[25] whose meaning is reasonably well settled. The provider exception of the Wiretap Act gives a provider the right to conduct reasonable, tailored monitoring of the network to protect the provider's property from unauthorized use and for other legitimate provider reasons, as well as to disclose communications intercepted.[26]

Thus, the seeming uncertainty attending the law is rather overblown.[27] There are, however, some real residual questions. The source of the ambiguity lies in the scope and frequency of the information sharing at issue. These provisions permit a "tailored" approach and may not necessarily be read to authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To interpret them so broadly might be inconsistent with the promise of privacy that undergirds the Wiretap Act and SCA. And yet, routine sharing may be precisely what is necessary to effectively protect the networks. Hence, though the statutory limitations are not as stringent as might be imagined, they do have some effect – and pity the service provider who is trying to determine when his permissibly "tailored" sharing becomes impermissibly "routine."

There are other possible answers of course. For example, both the Wiretap Act and the SCA have consent provisions permitting disclosure or interception in situations where the customer has consented.[28] Relying on these provisions, it would appear that service providers are authorized to collect, use, and disclose communications-related information whenever a subscriber has consented. To

---

[25] 18 U.S.C. § 2511(2)(a)(i).

[26] As a Department of Justice manual details, the provider exception to the Wiretap Act:

> grants providers the right "to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service." United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). . . . The exception also permits providers to monitor misuse of a system in order to protect the system from damage or invasions of privacy. For example, system administrators can track intruders within their networks in order to prevent further damage. See [United States v.] Mullins, 992 F.2d [1472,] 1478 [9th Cir. 1993] (need to monitor misuse of computer system justified interception of electronic communications pursuant to § 2511(2)(a)(i)).
> . . . .
> [P]roviders investigating unauthorized use of their systems have broad authority to monitor and disclose evidence of unauthorized use under § 2511(2)(a)(i), but should attempt to tailor their monitoring and disclosure to that which is reasonably related to the purpose of the monitoring. See, *e.g.*, United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975) (phone company investigating use of illegal devices designed to steal long-distance service acted permissibly under § 2511(2)(a)(i) when it intercepted the first two minutes of every illegal conversation but did not intercept legitimately authorized communications).

Searching and Seizing Computers and Obtaining Electronic Evidence Manual, ch. 4 (3rd ed. Sept. 2009), http://www.cybercrime.gov/ssmanual/04ssma.html.

[27] Section 314 of the USA PATRIOT Act, may also apply when the private-to-private sharing is done by a "financial institution" (as defined in 31 USC §. 5312(a)(2)). Such institutions are immune from liability for sharing information with each other when, broadly speaking, the information shared is done for the purpose of establishing or maintaining an anti-money laundering program. *See generally* 31 CFR *Part* 103.

[28] 18 U.S.C.§ 2511(2)(c) (Wiretap Act); 18 U.S.C. §2702(b)(3) (SCA).

be sure, there may be ambiguity in the terms of service of existing contracts, but there does not appear to be any barrier to cybersecurity information sharing arrangements if they are, ultimately, grounded on the affirmative, opt-in consent of a customer.[29]

Authorizing Sharing and Legal Uncertainty

The bills pending before Congress go a long way to relieve this uncertainty by explicitly authorizing cyber threat information sharing between private parties and from the private sector to the government. But merely authorizing information sharing will not be sufficient. Simply permitting the sharing will not generate the requisite private sector response if the private sector actor can anticipate adverse collateral consequences.

Why the Hesitation? -- On the private sector side, the reasons for hesitation are clear. Service providers (or more accurately the lawyers for service providers) are inherently cautious and want to avoid litigation and controversy at all costs.

Likewise, there may be good business reasons why a service provider might prefer not to risk collateral consequences such as privilege waivers and the discovery of proprietary information by competitors and critics. Seen in this light then, complaints about the law's ambiguity are also expressions of a desire to have the Federal government, by law, provide liability protection and relieve the service providers of the "ill will" that might attend such an amendment. Trying to avoid litigation and a difficult public relations battle are persuasive reasons for failing to act (though perhaps less so than real ambiguity), and they reflect rational business judgments that provide a good ground for legislation.

The private sector's argument for greater liability protection (and being "authorized" to do the right thing) seems to have carried the political day. The salience of the information-sharing issue was highlighted by the provisions of both the Lieberman-Collins and McCain cybersecurity proposals now pending before the Senate. Both bills clarify that private sector actors are authorized to share information about cyber threats or incidents with the Federal government and with each other. To address the private sector's concerns, the proposal would:

- Affirmatively authorize private sector actors to share information with the Federal government for the purpose of protecting an information system from cybersecurity threats or mitigating such threats;
- Provide private sector actors with civil and criminal immunity for sharing cybersecurity information with DHS; and

[29] There are other ambiguities in the law of lesser general concern relating to the Telecommunications Act of 1934, the Sherman Antitrust Act and, possibly, the Fourth Amendment. For purposes of brevity I will simply say that, as with the ECPA and the SCA the ambiguity is real, though it can be overstated. Perhaps more importantly, there is substantial, significant ambiguity from the application of State laws, many of which impose obligations and limitations that differ from those in the Federal domain.

- Preempt any inconsistent State or local law or regulation that would otherwise prohibit information sharing.

In each of these regards the information-sharing portions of the Lieberman-Collins bill and the McCain proposal closely track the general thrust of the proposal made by the Obama Administration last May.[30] Details, obviously, differ among the three proposals, but the overall thrust is much the same.

Freedom of Information Act Exemptions

Most saliently for this Hearing , both Senate proposals (and the Obama Administration proposal) also include provisions exempting private sector information shared with the Federal government from the ambit of the FOIA. In my judgment that exemption is both wise and essential. If you accept the premise that the cyber threat is real (and I recognize that some may not) then it seems to me that we must resolve any legal uncertainty in favor of enabling information sharing about threats and vulnerabilities. Essential sharing will not occur from the private sector if it is not relieved of the specter of liability and concern that disclosed information will be use adverse to their interests.[31]

The Lieberman-Collins and McCain proposals have, effectively, equivalent FOIA exemption provisions. Section 704(d)(1) of the Lieberman-Collins bill provides that any cyber threat information shared by a private entity with a federal cybersecurity exchange (the new information-sharing structure created by the bill), shall be "exempt from disclosure under section 552(b)(3) of title 5, United States Code, or any comparable State law." Likewise the McCain proposal (in section 102(c)(4)), says that any cyber threat information shared with a Federal cybersecurity center, "shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records." To emphasize the intent of the exemption, the McCain bill further provides (in section 102(c)(5)) for a specific exemption from the OPEN FOIA Act of 2009.[32]

Notably, the consensus about the need for a FOIA exemption is bi-cameral. The Rogers-Ruppersberger bill, H.R. 3523, also provides that any cyber threat information shared with the Federal government is exempt from disclosure under the FOIA. And the Lundgren bill (H.R. 3764) says that information shared with the to-be-created National Information Sharing Organization will, likewise, be exempt from disclosure under FOIA. Not only is the consensus bi-cameral, it crosses branches of government -- the

[30] The language is in §245 of the draft submitted to Congress by the Administration on May 12, 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

[31] Much of what I say in this section about the FOIA exemption is also applicable to arguments regarding privilege waiver provisions and prohibitions on the regulatory use of disclosed information.

[32] Section 102(c)(5) requires that information disclosed "shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records."

Obama Administration cybersecurity proposal, in section 245(f) also contains an FOIA exemption that mirrors that in the Lieberman-Collins/McCain/Rogers-Ruppersberger and Lundgren proposals.

Now, some may argue that much of the concern can be answered by the use of existing FOIA exemptions, rather than the blanket provisions of the two pending bills They point out that FOIA already has a bevy of exemptions for national security (5 USC 552(b)(1)), privacy (552(b)(6) and (7)), internal agency decision-making ((b)(5)) and law enforcement ((b)(7)), and suggest that those provisions are sufficient. In my judgment they are inadequate to the task.

First, despite the best intentions, the application of exemptions will, inevitably create greater uncertainty than an absolute prohibition. As the *Milner*[33] case from 2011 demonstrates powerfully, even interpretations of FOIA that have been settled law for a significant period of years are subject to reinterpretation. This potential for ambiguity in the application of FOIA strongly counsels in favor of a blanket exemption .

Second, it is by no means clear whether cybersecurity threat and vulnerability information will fit within one of the existing FOIA exemptions. One can readily imagine types of information (protocol and packet routing information or web-site access logs) that fits in none of these pre-existing categories.

Third, and perhaps more importantly, the application of FOIA in this context seems to me too turn FOIA on its head. The purpose behind the FOIA is to ensure the transparency of government functions. Thus the main ground of a FOIA request is to seek information from the government about the government and its operations. Here, the FOIA exemption contemplated is in relation to private sector information that is not otherwise in the government's possession. We seek the voluntary (*not* compulsory) sharing of this information in order to foster the creation of a clear and manifest public good. But for voluntary agreement of the private sector actors to provide the cyber threat information in the first instance the information would not be in the government's possession and thus not subject to disclosure.

Private sector actors, rightly, would see the absence of an FOIA exemption as a form of government hypocrisy – we need this information, says the government, badly enough that we are asking you to provide it for the common good; but not, says the government in the next breath, so badly that we are unwilling to prevent that information from being shared with other private sector actors who (as your competitors or as your litigation adversaries) might wish you ill.

This, it seems to me, undercuts the very thesis of these information-sharing proposals. If you think (as I do) that sharing of cyber threat and vulnerability information is the most effective (and most cost-effective) way of significantly enhancing the cybersecurity of America's critical infrastructure you cannot, in the same act, turn around and say that the threat information you provide becomes, *pro tanto*, public information.

[33] *Milner v. Dept. of the Navy*, __ U.S. __ (2011), No. 09-1163, http://www.supremecourt.gov/opinions/10pdf/09-1163.pdf.

Finally, let me close this analysis by noting that none of this is to diminish the significance of the FOIA, generally. Transparency is a fundamental and vital aspect of democracy. Those who advance transparency concerns often, rightly, have recourse to the wisdom of James Madison, who observed that democracy without information is "but prologue to a farce or a tragedy."[34]

Yet Madison understood that transparency was not a supreme value that trumped all other concerns. He also participated in the U.S. Constitutional Convention of 1787, the secrecy of whose proceedings was the key to its success. While governments may hide behind closed doors, U.S. democracy was also born behind them. It is not enough, then, to reflexively call for more transparency in all circumstances. The right amount is debatable, even for those, like Madison, who understand its utility.

What we need is to develop an heuristic for assessing the proper balance between opacity and transparency. To do so we must ask, why do we seek transparency in the first instance? Not for its own sake. Without need, transparency is little more than voyeurism. Rather, its ground is oversight--it enables us to limit and review the exercise of authority.

In the new cyber domain, the form of oversight should vary depending upon the extent to which transparency and opacity are necessary to the new powers authorized. Here, the proposed legislation would exempt information supplied by businesses regarding cyber attacks from public disclosure. Supplying this information to the government is vital to assure the protection of critical infrastructure. More importantly, allowing public disclosure of such information is dangerous – identifying publicly which cyber threats are known risks use of that information by terrorists and, in turn, draws a roadmap of which threats are not known. Thus, complete transparency will defeat the very purpose of disclosure and may even make us less secure.

What is required is a measured, flexible, adaptable transparency suited to the needs of oversight without frustrating the legitimate interests in limiting disclosure. Here, the public disclosure through FOIA should be rejected in favor of a model of Congressional and Executive Branch review (for example, random administrative and legislative auditing of how the government is using the information provided) that will guard against any theoretical potential for abuse while vindicating the manifest value of limited disclosure.

In short, Madison was not a hypocrite. Rather, opacity and transparency each have their place, in different measures as circumstances call for. The wisdom of Madison's insight--that both are necessary--remains as true today as it was 225 years ago.

[34] I first wrote about the thoughts in these concluding paragraphs in Rosenzweig, Calibrated Openness, Harv. Int'l Rev. (Summer 2004).