Issue Analysis

Preventing Identity Theft and Data Security Breaches:

The Problem With Regulation

by Clyde Wayne Crews Jr.

and Brooke Oberwetter

May 9, 2006

Preventing Identity Theft and Data Security Breaches: The Problem With Regulation

By Clyde Wayne Crews Jr.

and Brooke Oberwetter

Executive Summary

Numerous high-profile cyber-attacks have spawned intense calls for government intervention into information security practices. Tired of the many online threats—including identity theft, data security breaches, and destructive viruses—the public and even some industry representatives are increasingly open to using government regulation to deal with electronic security issues.

Several bills introduced in Congress address what is popularly perceived as a matter of market failure in the area of cybersecurity: According to some, imperfect information, externalities, and a lack of proprietary incentives in the Internet "commons" will perpetually leave the industry incapable of solving its own problems. A sampling of the legislative proposals includes plans to require reporting to customers when a data breach has occurred, regardless of the severity, and to mandate annual security audits not unlike the financial audits required by the Sarbanes-Oxley legislation.

But are the problems that legislative solutions can address really market failures, or has the industry simply been slow to adapt to emerging threats? The problems identified by proponents of regulation could all be fixed far more effectively and efficiently with market solutions—among them, liability, insurance, third-party monitoring and ratings, and property rights—than with government mandates. Thus, claims of market failure are unsubstantiated. Addressing cybersecurity, then, is not a question of how best to regulate businesses that are victims of cyber-attacks, but a question of how best to put market mechanisms into Internet and information technology operations to create incentives for improved security.

Improving information security will require a reconsideration of some of the basic features of the Internet, specifically the ease of anonymity and the open, public nature of the medium. Improvements can also be induced in the market by making individuals and companies internalize the costs of lax security practices and letting them reap the benefits of good practices through both lower insurance premiums and higher industry rankings.

Government solutions, on the other hand, will tend to disincentivize honesty and cooperation among industry players in the long term, leading to even greater problems of imperfect information. Intervention can also interfere with prices, meaning a less efficient allocation of resources. In addition to economic inefficiency, regulations can define industry standards down and reduce innovations in the field of cybersecurity, leading to lower levels of security than we have now.

The threats against consumers and companies are numerous and the impulse to regulate is strong, but Congress would be well advised to avoid legislation that is rigid in nature and will likely prove ineffective. The best thing lawmakers can do in the name of information security is apprehend and prosecute criminals, realizing that it is the private sector that occupies the territory from which a successful defense against attacks on hardware and information can be mounted. The need to preserve a dynamic market role can be summed up in a single Cybersecurity Commandment:

> Do not take steps in the name of security that make it:
>
> (1) impossible to liberalize or deregulate infrastructure or
> (2) impossible or undesirable to self-regulate.

Introduction: The Growing Impulse to Regulate Data Security

[I]f we as an industry don't solve the problem [of information technology security], you're likely to see a rash of government regulation crop up.[1]

—Symantec Corp. Chief Executive John Thompson

Help yourselves. Fix security soon, or Washington will do it for you….[U]nless more effort is put into computer security by industry, Congress is going to want action…Not because it might be effective, but because they need to do something.[2]

—One lobbyist's warning to assembled corporate computer security representatives

Identity theft, data security breaches, viruses and other online insults are spawning intense calls for government intervention. Numerous high-profile cyber-attacks or scams have occurred at database companies like ChoicePoint and LexisNexis, as well as at universities, banks, and other firms. All of these instances have aided in putting cybersecurity on the national agenda.

Proposed remedies lean toward government action. In 2003, Rep. Adam Putnam (R-FL), chairman of the House Government Reform Technology Subcommittee in the 108th Congress, warned corporate America: "If there is a major cyber attack … there will be major legislation that takes a much more aggressive stance...and [the industry is] not going to be able to say 'boo' about it. So it behooves them to get in on the front end of this rather than being run over by the next crisis."[3] Taking a less encouraging tone, some policy experts in the field openly reject the idea that industry can combat the cybersecurity problem without government intervention. As James Lewis of the Center for Strategic and International Studies points out, "Cybersecurity is too tough a problem for a solely voluntary approach to fix…Companies will only change their behavior when there are both market forces and legislation that cover security failures."[4]

With the public tired of electronic interruptions and privacy invasions, there is increasing openness to well-intended legislative solutions; this is, after all, the era of the national Do Not Call Registry and anti-spam laws. Unfortunately, legislative solutions to technological problems may either overreach or not work at all. The Do Not Call Registry, for example, has raised issues of free speech and other legal challenges, while spam defiantly continues to overwhelm inboxes despite the 2004 legislation designed to combat it.

Cyber-attacks pose even greater threats to privacy than spam and telemarketers, and it is in this heated environment that Washington and many state governments are now considering data security proposals. But the impulse to find regulatory solutions is not exactly new. Even before the September 11, 2001 terrorist attacks, a report by the D.C. law firm Sidley Austin Brown & Wood noted: "Although a move toward comprehensive regulation of Internet and computerized data service providers would represent a sharp deviation from current policy, where only banks, health care providers, and other companies that store inherently sensitive types of data face government regulation, further regulation or creative judicial theories cannot be ruled out."[5]

Stronger evidence of the growing push for regulation came in September 2002, a few months before the final report on The National Strategy to Secure Cyberspace was released by the President's Critical Infrastructure Protection Board. A draft report issued by the board[6] was met with largely negative reviews: it didn't call for enough regulation and was thus toothless;[7] it was "astoundingly without gravity;"[8] it was simply "sixty pages of nothing."[9] Bruce Schneier, a leading security expert and usual critic of government regulation of encryption, proclaimed, "If the U.S. government wants something done, they should pass a law. That's what governments do."[10] Security expert Fred Avolio called for Internet Service Providers (ISP) regulation, such as requiring user authentication for access.[11] The InfraGard partnership of private security professionals rejected the report's guiding principle to "Avoid Regulation," holding that market forces were not adequate.[12] Alan Paller, of the SANS Institute (SANS stands for SysAdmin, Audit, Network, Security) argued: "The administration says computer security is like auto safety, that everyone will keep their systems safe because it's in their best

interests to do so. But that's not true, and it just doesn't happen."[13] Security systems expert Marcus Ranum was even bolder in his call for regulation: "Personally, I am comfortable with our government bending a few peoples' noses out of joint."[14]

Though the final National Strategy to Secure Cyberspace did emphasize private solutions, it strongly hinted at the possible need for future regulation:

> In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government response is most appropriate and justified. … [A] government role in cybersecurity is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems; cases in which governments operate in the absence of private sector forces; resolution of incentive problems that lead to under provisioning of critical shared resources; and raising awareness.[15]

It also offered a final piece of high-profile ammunition for federal jurisdiction over cybersecurity regulation: "As appropriate, the executive branch may ask Congress to enact legislation to advance this strategy."[16] More recent criticism of the inadequacy of private sector efforts comes from Mark Rasch of Solutionary Inc. Rasch said: "The challenge is to skew the marketplace . . . to push either with regulations or the threat of regulations, liability or the threat of liability, standards or the threat of standards."[17]

Identity theft, data security breaches, viruses, and other online insults are spawning intense calls for government intervention.

The prodding from the National Strategy report, the demand for government action from key industry representatives, and the mounting public concern about identity theft were not wasted on Congress. In 2004 and 2005 there were multiple congressional hearings—some hot on the heels of high profile data-breach cases—about the steps companies were taking to curb threats posed to consumers by would-be identity thieves and hackers. Several bills were introduced, including proposals to phase out the use of Social Security numbers, require reporting to customers when a data breach has occurred,[18] create an Office of Identity Theft as part of the Federal Trade Commission (FTC), and regulate multiple aspects of how companies collect and maintain consumers' personal data.[19]

Although most of the bills introduced in both the House and the Senate in 2004 and 2005 were left to languish in committee, several pieces of legislation are still under consideration. Most prominently are H.R. 4127 and S. 1789. The former, the Data Accountability and Trust Act (DATA) went through markup, was reported to the full House Committee on Energy and Commerce in late March 2006, and is awaiting a full committee vote, and a possible subsequent House vote. H.R. 4127 allows for the FTC to regulate the security protocols of any commercial outfit that "owns or possesses data in electronic form containing personal information." "Personal information" is fairly narrowly defined, however, referring only to a consumer's first and last name plus either their Social Security number, drivers license or other state ID number, or financial account number. The bill also creates requirements for "information brokers," firms that collect and maintain databases of personal information on individuals who are not their direct customers. Finally, DATA would move to supersede existing state laws dealing with information security and require compulsory notification of consumers for any breach that establishes a "reasonable basis to conclude that there is a significant risk of identity theft."[20] An amendment added during markup also included a provision to allow enforcement by state attorneys general via civil action in cases where the AG believes "that the interest of the residents of that state has been or is threatened or adversely affected by any person who violates" the Act by Sen. Arlen Specter (R-PA) and Patrick Leahy (D-VT).[21]

In the Senate, S. 1789, is a likely candidate for further action. The bill has three main functions. The first is to strengthen criminal laws by enhancing punishment for fraud and unauthorized uses of "digitized or electronic" personally identifiable information, making such criminal activities predicate offenses under the

Racketeer Influenced and Corrupt Organizations (RICO) Act. To enable enforcement of those criminal penalties, the bill requires breach disclosure for a breach of any size and grants the Secret Service investigatory authority. The second function is to regulate "data brokers," which are defined in essentially the same way as H.R. 4127's "information brokers." The third, and most applicable function to the issue of cybersecurity, is to regulate all businesses "engaged in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of" electronic personal information on more than 10,000 people. The bill requires companies to implement comprehensive security plans that include safeguards identified by the FTC and continually assess vulnerabilities and possible damages; mandates notification of all customers whose information has been breached if there is a significant risk of harm and requires that breaches deemed *not* harmful be disclosed to the Secret Service for further investigation. It also imposes further requirements on businesses based on the size and scope of breaches.[22]

Many of the problems with provisions of these bills are discussed in following sections of the paper. But what is not addressed directly are the problems that can come about purely through the vague terminology used in crafting legislation, most specifically problems of implementation. These problems can be particularly acute in regulations that deal with technologies with which lawmakers have only minimal familiarity. Both bills, for example, place significant regulatory burdens on data, or information brokers. But as Declan McCullagh, political correspondent for CNET News and editor of the politics and technology website PoliTech, pointed out in response to Specter-Leahy, the vaguely defined targets of those regulations could give regulators unintended powers:

> [T]he definitions could cover, for instance, news organizations (many news sites arguably provide personal information on thousands of people, and People magazine's Web site certainly does). How about popular blogs that have thousands of registered users? Search engines? Google's phone number finding service? Libraries? Email service providers? Alumni organizations for schools? Charities, like Golden Gate National Parks Association? What about universities, especially in terms of all the applications they get? Sweepstakes companies? I wonder if probable supporters of this bill—like the ACLU and EPIC—would enjoy having to follow all these complicated procedures (with the penalty of fines or prison terms if they don't).[23]

Market Failure—or Government Failure?

Heck, despite being libertarian in nature, I'm all for a government crackdown.

—A participant in online discussion on virus attacks, quoted in the *New York Times*.[24]

The better-articulated arguments for information security regulation tend to point to *market failure*. The impulse to regard cybersecurity vulnerabilities as market failures is understandable: There is difficulty in coordinating and satisfying conflicting, legitimate interests online. More central to the market failure argument, however, is the fact that so far, market-based mechanisms that would allow individual firms to fully internalize the benefits of securing networks and data (or force them to fully internalize the costs of their own lax security) have not emerged.

In congressional testimony on broader questions of critical infrastructure security, Peter Orszag of the Brookings Institution argued: "Private markets, by themselves, do not provide adequate incentives to invest in homeland security. A mixed system of minimum regulatory standards, insurance, and third-party inspections would better harness the power of private markets to invest in homeland security in a cost-effective manner."[25] Bruce Schneier argued: "Security is a commons. Like air and water and radio spectrum, any individual's use of it affects us all. The way to prevent people from abusing a commons is to regulate it. Companies didn't stop dumping toxic wastes into rivers because the government asked them nicely. Companies stopped because the government made it illegal to do so."[26]

However, there is no reason why information security—or even "air, water and radio spectrum" for that matter—should be a "commons" requiring government management. Market alternatives to regulation that require network operators, careless individuals, and other participants to internalize the costs of substandard security—or internalize the benefits of better security—include contracts, property rights, and liability. Orszag, still speaking on the broader issue of securing critical infrastructure, holds that:

> "The costs of allowing terrorists to obtain access to [hazardous materials] are generally not borne by the facilities themselves: The attacks that use the materials could occur elsewhere. Such a specific negative externality provides a compelling rationale for government intervention to protect highly explosive materials, chemicals, and biological pathogens even if they are stored in private facilities."[27]

If, as Orszag argues, the costs are not "borne by the facilities themselves," this raises a critical question: *Why not*? Why can an enterprise store massive quantities of hazardous substances without liability insurance? Was there a government-granted waiver of liability? Such protections from costs are not market failures, but policies that deliberately shield firms from having to internalize negative externalities related to security threats. They are *government failures*. One can only assume that if minimum standards of cybersecurity set by government regulators are met, network administrators and firms that maintain sensitive personal data will be similarly shielded from liability in the event of an attack.

In a world of near-total connectivity, it is all too easy for unmotivated individuals or institutions to externalize the costs of their inadequate cybersecurity measures. Clearly, the unwillingness of some to upgrade online security causes grief to many others—a classic case of a negative externality of a market behavior. But the ability to externalize the costs of one's own laziness need only be a transitional artifact of the Internet's original design, which was based on limited connectivity among trusted parties; in the early Internet era cybersecurity was only a minor issue.

There is no reason why information security should be a "commons" requiring government management.

In the age of global connectivity, however, network administrators, cybersecurity firms, businesses that collect personal data, and individual users are all acutely aware of the security risks, and there is increasing demand to curb those risks. There's no reason to believe that the market will fail to adequately register and satisfy that demand if given the opportunity. As discussed in detail below, market alternatives and incentives can increasingly encourage market participants to internalize the risks of their online behavior that they would otherwise foist onto others. And, just as firms regularly police their up and downstream partners in product and service markets, they will increasingly do so for security practices, mitigating the need for intrusive government oversight.

Given government's own security shortcomings, it is difficult to envision how it would improve upon alleged market failure. Consider, for example, a government-certified firewall: What happens when the approved firewall fails? What is the security downside to having a government-determined firewall standard rather than leaving the field competitive? Markets, clearly, can and do develop and improve firewalls without government intervention. Regulation—and reductions in liability that would doubtless accompany compliance—would replace private incentives to outperform competitors with an industry-wide incentive to adopt subpar technologies: a perpetual a state of government failure. Conditions such as traffic congestion, emissions, and product certification—initially deemed market failures that warranted regulatory responses—often become recognized as transitory, or at least surmountable.[28]

Traditionally, market failures are attributable not just to externalities, but also to imperfect information and transaction costs. But in information technology, barriers to information and transaction costs are low given the nature of networked communications. In order to overcome traditional market failure, government would

essentially need to *invent* the kind of communications system the online realm now provides. It is ironic that government now claims that the existence of the Internet and networked communication is itself a source of market failure because of cybersecurity risks; policymakers should recognize instead that information technologies help *overcome* traditional market failures. For example, standardization across computer platforms, such as Microsoft's Windows—although often blamed for the spread of viruses—enables quick learning and lowers training costs.

The market's growing pains do not signify an inherent inability of the cyber-sector to protect itself, nor do they represent market failure, particularly when compared to the government failure that would occur through regulation. Government's shortcomings are all too frequently dismissed in favor of regulatory redress when private-sector weaknesses are exposed. But regulations that will divert resources from improving security mechanisms, as well as rules that interfere with private assessments of relative cyber-risks, will make future course corrections much more difficult.

Government Solutions in Search of Problems

Despite the shakiness of market failure arguments as applied to the cyber-sector, there's no dearth of regulatory proposals that attempt to rectify the perceived problems. Marcus Ranum, the expert who advocated the government's disjointing a few noses, suggests outlawing the selling of computers that don't come with fully-licensed antivirus and firewall software pre-installed.[29] An expert at Qualys, Inc. favors policies encouraging automated security-patching tools.[30] Oracle representatives proposed in congressional testimony that government review and certify certain software.[31] Still, other proposals would hold chief information officers liable for network security, particularly for high-profile hacking incidents,[32] and make board members liable for security policies.[33] Even the idea of limiting anonymity on the Internet has been raised.[34] Already in play is government-funded cybersecurity research.

Other ideas have included restrictions on company use of wireless networks, mandatory contributions to a government computer security fund,[35] improvements in wireless hardware security, and requirements that ISPs furnish customers with firewall software.[36] Proposals for mandatory security testing have also been considered.[37] One article in *CNET News* listed several proposals: holding parties—ranging from inattentive network administrators to software makers—liable for security breaches; requiring information-sharing between government and business; requiring that the Internet's governing body (the Internet Corporation for Assigned Names and Numbers) provide security guarantees; requiring that ISPs improve screening capabilities and provide virus protection; and calls for more federal involvement in the formulation of Internet protocols and standards.[38] Still other ideas include backup power supply mandates and security mandates for the Web servers that host Internet sites.[39] In one extreme reaction, the idea of professional licenses for software engineers—like a medical license—was even floated,[40] as if such uniformity of training were desirable or even relevant to the myriad programming needs of the future.

Mandatory Disclosure: Blaming the Victim

Breach-disclosure and other reporting mandates possess the most traction, although there is little broad consensus on specific breach-disclosure requirements. Controversy exists over what qualifies as "reasonable basis" for triggering disclosure, who is responsible if the targeted company's database is hosted by a third party, the wisdom of publicizing relatively minor breaches, and the merits of alerting consumers instead of law enforcement.[41] Forced disclosure may also conflict with the Bush Administration's assurances that the names of computer crime victims would not be publicized, so as to encourage victims' reporting to the authorities.[42] Although California has already passed a disclosure law stipulating that companies failing to alert consumers about Social Security number and other private data breaches are subject to lawsuit,[43] a national program could create considerable noise for investors, managers, and customers given the regularity of attempted hacks. It would not be unlikely to see a boy-who-cried-wolf effect, where consumers simply grow less and less concerned with each alert.

Often, few outside a company know of a security breach until the hacker publicizes it. Yet companies may be disinclined to report for non-sinister reasons, such as lack of severity, or uncertainty over whether the breach should be publicized or rather reported to authorities.[44] The disinclination to report is occasionally regarded a "failure" that the government should repair legislatively. For example, in August 2002, Federal Deposit Insurance Corporation guidelines required financial institutions to warn consumers about any unauthorized access that could enable harms such as identity theft.[45] But many firms had already decided internally to make such disclosures.[46] Competitive pressures will force disclosure when it makes sense, and security-savvy consumers may even begin to demand information about disclosure policies as a matter of course in selecting companies to whom they'll give their business.

Also controversial are similar questions regarding disclosure of newly uncovered software flaws. One promising proposal to address software vulnerabilities (and data breaches) is voluntary industry funding of a neutral third party—rather than a government agency—to inform developers about vulnerabilities, and impose deadlines for fixes before flaws or breaches are publicized.[47] Calls for government regulation clearly indicate that there is a market demand for such a service, but unlike a mandatory regulatory process to which all firms must adhere, a firm's failure to participate voluntarily will signal questionable product or service quality. Such market-based remedies create incentives to self-report, rather than incentives to hide flaws. Market-based remedies would also eliminate the somewhat paradoxical nature of disclosure legislation, which levies legal penalties against companies for having been robbed. Unless negligence is a factor, a company hasn't committed a crime by being robbed, whether its databases were invaded or its software exploited. *The invader merits punishment, not the victim*.

Requirements for more universal reporting by all companies on data security policies—not just those that have experienced a break in—would likely follow any disclosure legislation enacted. One proposal already considered by White House and Department of Homeland Security analysts was mandatory annual public disclosures of cybersecurity efforts by businesses, with Y2K-style audits and reporting requirements.[48] Although mandatory public disclosure was intended to encourage voluntary increases in cybersecurity efforts—at least keeping with the *National Strategy*'s optimism about markets in spirit—it was probably inevitable that the flood of proposals for regulation caused some officials to abandon the report's skepticism of mandates. A broad reporting proposal was echoed by former National Infrastructure Protection Center (NIPC) head Michael Vatis, who called for "soft" regulatory requirements that cybersecurity plans be reported in public companies' financial filings with the Securities and Exchange Commission (SEC).[49] (Along with mandatory reporting, Vatis also called for requirements that private companies disclose breaches and for enforcement of best security practices.[50]) Firmly in the market failure camp, Vatis told *The New York Times*: "The government has essentially relied on the voluntary efforts of industry both to make less-buggy software and make systems more resilient. What we're seeing is that those voluntary efforts are insufficient."[51]

Calls for public disclosure on cybersecurity practices bear a striking resemblance to the calls for financial accountability in the wake of Enron's collapse and various other corporate accounting scandals. The Sarbanes-Oxley financial accountability legislation, signed into law in July 2002, requires that companies report to the SEC on accounting practices and that corporate officers vouch for the numbers. Widely regarded as onerous, Sarbanes-Oxley provides a likely preview of any cybersecurity audit-and-reporting proposals, with business taking a hit. Speaking before a House Government Reform subcommittee, a Symantec security executive seemed to indicate as much when he called for upper-management accountability on cybersecurity efforts by invoking the financial accountability legislation as a model: "[Sarbanes-Oxley] makes no mention of the importance of protecting the information systems that produce the data used in the financial management process…Only when cybersecurity is treated with the same attention as the protection of physical and financial assets can we enable the necessary cultural change and focus enough attention and resources to truly address the cyber-threat."[52]

In 2003, Rep. Adam Putnam proposed cybersecurity reporting legislation mirroring Sarbanes-Oxley's requirements: Public corporations would be forced to undergo a security audit—for which upper-management

would presumably vouch—and present the results to the SEC.[53] But, notably, unlike Y2K reporting, such mandates would be ongoing, *not a response to a one-time crisis*. But pause to consider how much credit Y2K reporting mandates should get for the fact that our computers, for the most part, emerged unscathed into the year 2000. Companies didn't need government prodding to look out for bottom lines—businesses do that naturally. Moreover, ongoing reporting requirements violate basic principles of justice by burdening *all* firms, not just those that engage in criminal or negligent behavior. It is uniquely invasive to force honest members of the business community to sign a sworn statement certifying that an audit has occurred and that a third party verified it. Unfortunately, Putnam's legislation was criticized merelyover the appropriateness of the choice of the SEC for the oversight role, [54] not the appropriateness of treating company representatives like schoolchildren.

Unfortunately, a CEO-certified security checklist, like the Department of Homeland Security's (DHS) color-coded threat level advisory system,[55] can quickly become meaningless noise. If a breach occurs under the new regulations, it is unlikely that regulators who imposed the ineffective and diversionary system in the first place would be held accountable. Also, it is equally unlikely that companies who had followed the letter of the law would be subject to liability. Under such a system, the only possible response to a high-profile cyber-attack would be more power for government officials and more ineffective and burdensome legislation.

The best way to prevent attacks in the cyber-sector in the first place is by letting market institutions like liability and insurance evolve in response to quickly emerging threats, business needs, and consumer demands.

It is difficult for anyone whose services are connected to a public, open network like the Internet to offer airtight security guarantees, and regulation does nothing to make it easier. Moreover, legislation geared towards regulating American business practices will be of limited use on a globally connected network. Rather than harassing legitimate businesses, government resources would be much better spent dealing with offenders who target Internet users, such as the Love Bug virus creator, who was tracked to the Philippines but never prosecuted. The best way to apprehend and punish cyber-criminals is through coordinated government action. But the best way to prevent attacks in the cyber-sector in the first place is by letting market institutions like liability and insurance evolve in response to quickly emerging threats, business needs, and consumer demands.[56]

Private Sector Experimentation and Innovation: Incentives Matter

[T]he best way to address the threat to the Internet is private effort. The government's role is to stay out of the way of the people who created it and manage it.[57]

John Tritak, former director of the Critical Infrastructure Assurance Office

Coordination across Market Quarters

Most cyber-nuisances stem from two of the Internet's most touted features: openness and ease of anonymity. In the future, cybersecurity will depend on a cross-fertilization of ideas from various subgroups of the cyber-sector for controlling the negative effects of problems that arise from those features. Data breaches and identity theft share features with irritants like email spam and the piracy of digital content in that all are facilitated by Internet openness and the ability to hide one's identity online. Also, the distinction between more sinister, criminal cyber-attacks and more benign—though certainly disruptive and annoying—cyber-nuisances like spam grows increasingly blurry: Email spam delivers viruses and recruits new, unprotected computers in extending the damage,[58] and phishing scams use elements of spam and piracy—such as stolen corporate logos—to gather

sensitive personal data about unsuspecting Internet users. The lesson for industry is that solutions proposed for curbing one cyber-problem may very well also be useful in addressing other problems.

One possible fix for dealing with both spam and piracy is the introduction of a tiered pricing structure for network use, which would address some of the problems associated with Internet openness. Network access is often structured as an all-you-can-eat buffet with a monthly flat rate for all the access you want. With broadband and cable access fast replacing dial-up, many users are connected all the time. Though consumers tend to prefer the ease and consistency of fixed fees,[59] such a structure incentivizes pirates and spammers to get the most bang for their buck, to pirate as much content or send as much spam as possible. Without a tiered structure of payment, both spam (getting stuff) and piracy (taking stuff) are likely to drive access and usage prices ever-higher for everyone's service: Average-volume users essentially subsidize spammers and pirates. Without legislative prodding—or rather in addition to the largely ineffective laws against spam and piracy already on the books—companies will experiment with introducing tiered pricing structures for a variety of Internet services.

On the anonymity issue, columnist Larry Seltzer notes that the technicians involved in controlling spam point to the reigning Internet protocol (called SMTP) as a source of the problem. Tonny Yu of Mindshell, a spam-filtering software company, suggested a gradual move away from SMTP to a system that verifies senders' identities with a certification mechanism and certifies mail servers to enable trustworthy email. Mechanisms to flag unusually high-volume mail senders and limit the number of emails that a single user can send per second can also help reduce spam.[60] Upgrades to Internet "plumbing" to verify senders and limit individual email capacity would address spam and broader information security concerns that urgently need to be addressed.

Ironically, after government action failed to reduce spam, there are now calls for government to prevent private action from succeeding as well.

In another example of solutions from within the industry, network providers have discovered that distributed denial of service attacks (deliberately overloading servers by sending repetitive requests) can be combated by employing puzzles that computers must solve to gain access to a targeted website; this would occupy the processing capability of the querying computer and limit the number of repetitive requests that could be sent to a "victim" site.[61] By imposing costs on the sender in the form of consumed CPU cycles, an attack could not progress unimpeded. Puzzle solving has been investigated as a means of dealing with spam as well; messages don't go through until the sender's computer is forced by the recipients' computers to perform a mathematical exercise, making the process of simultaneously sending thousands of uninvited emails an untenable proposition. Again, cross-fertilization of ideas for combating problems is apparent.

Solving problems by finding innovative ways to overhaul how the Internet works is far beyond the capabilities of regulators, but the market is already providing some gradual changes. Most notably, industry giant America Online (AOL) announced in early 2006 that it would implement certified email, which combines elements of both tiered pricing and sender certification. Certified email, provided by Goodmail Systems, would require organizations that send bulk email to pay a small fee for each message (a fraction of a cent) to bypass spam filters and let AOL email users identify mail from trusted and accredited senders.[62] Many business and advocacy groups want to prevent AOL from charging to ensure email delivery,[63] and at least one lawmaker, California State Sen. Dean Florez, is drafting legislation to prevent email "toll booths," which he plans to attach to a larger "net neutrality" bill.[64] Ironically, after government action failed to reduce spam, there are now calls for government to prevent private action from succeeding as well. But pricing experiments, although controversial in the short term, are crucial for signaling the market demand for cybersecurity, network use, and a host of other Internet services. Tiered pricing might also need only be a temporary fix that constrains Internet nuisances while technological advances work on ways to fully eliminate them.

In terms of more serious cybersecurity issues, one goal is preventing the spread of destructive applications through email. Arguing for a particularly strong remedy for the damage caused by executable attachments, Christopher Wysopal of the Organization for Internet Safety and @stake, Inc. testified before Congress:

> "All email programs need to be designed to not allow executable content to be sent or received. It is just too dangerous. …Older Email programs that allow this should be considered unfit for use on the Internet and eliminated. Eradicating executable attachments from the Internet will eliminate most email viruses."[65]

Less stringent remedies would prevent computers and email programs from executing code only from unauthenticated sources, the authentication mechanism being another product of cross-fertilization of ideas across sectors. The balance between demand for ease of use (by allowing code to automatically execute) and demand for security is shifting in favor of security. Richard Pethia of CERT noted:

> "There is nothing intrinsic about computers or software that makes them vulnerable to viruses. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow that code to be executed without constraint on the machine that received it. Unconstrained execution allows program developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack."[66]

Microsoft's newest version of the Windows operating system is being specifically designed with safeguards to prevent "unconstrained execution" of unauthorized code and other new security features, and other software makers are doing the same. The marketplace has clearly woken up to the problem.

Companies Have Incentives to Correct Problems on Their Own

Experimenting with different defenses against threats will affect the entire cyber-infrastructure, sometimes in unanticipated and undesirable ways. Overly aggressive filters that accidentally shut out non-spam email or block inoffensive domains are one such glitch in the remedies already available. Even so, mistakes that emerge from voluntary, private effort will be far easier to correct than mistakes that result from ill-considered legislation. Networks and businesses can easily detect and respond to any unintended consequences of new solutions, and they have an incentive to do so quickly and effectively. But when unintended consequences result from government regulations, it's difficult to get quality information into the hands of decision makers, and harder still to draft, adopt, and implement necessary corrections.

Market forces will also provide incentives for constant improvements in online security, incentives that regulation simply can't create. Consumers will increasingly seek out and patronize vendors that meet their demands for better security and privacy assurances online. Applications which are perceived as less secure, such as wireless networking and instant messaging, will require substantial security improvements to become—or to remain —viable in the marketplace. And service providers that develop bad reputations on security matters will either improve their quality or go out of business. An impediment to widespread adoption of voice-over-Internet protocol (VoIP) service, for example, has been the vulnerability of the network.[67] Government interference cannot replace technical know-how, and it can even stymie innovation by locking in government standards that soon become outdated.

The market failure school claims that consumers and vendors will fail to adequately internalize the costs of providing a safer cyber-atmosphere by refusing to pay higher prices for security. Those claims carry increasingly less weight, however, as Internet attacks become more pernicious and identity theft becomes more common. Meanwhile, arguments pointing to the market failure of imperfect information in order to justify government intervention warrant similar skepticism. As economist Arnold Kling notes:[68]

> Economists are wary of overriding the market decisions of consenting adults…One rationale for government intervention in software is that buyers are uninformed, [but the] people with the strongest incentive to make the right choice in software purchasing are the decision-makers at large private corporations. If the cost of Microsoft's security flaws is greater than the benefits of continuity and integration, then private corporations ought to be able to figure this out and change their buying habits. If they do not change their buying habits, then … government ought to be really cautious about assuming that it has better information.

The unknown effects of new discoveries or new technologies on the existing order can lead to misplaced appeals to authority to relieve uncertainty. Uncertainty is the impetus for government intervention into cybersecurity, and, as discussed previously, it was the catalyst for corporate accounting regulations. Writing about the "instinctive preference for hierarchic control" in response to uncertainty, Fred Smith, founder and president of the Competitive Enterprise Institute, might just as well have been describing cybersecurity risk management:

> [Centralized regulation] weakens the evolving competitive forces that promise to make such disasters [like Enron] less likely in the future. Indeed, political intervention in response to economic mishaps often increases risk from moral hazard—the tendency of individuals to act in a riskier fashion if they believe any costs of such risks will be borne by others…. These interventions undermine competitive pressures for prudent risk taking…Also, we weaken the incentives of the parties most knowledgeable about risks to innovate.[69]

Market forces will also provide incentives for constant improvements in online security, incentives that regulation simply can't create.

Seeking Best Practices: Everybody's On Board

Criminals routinely cooperate to exploit stolen identities, wreaking havoc on commercial interests like credit card systems. Computer and communications industries must cooperate as well. If any good can come of the federal government's recent attention to cybersecurity, it will be that it has served as a wake-up call on the need to combat cyber-attacks through industry-wide effort. Authenticating users accessing critical online networks (through biometric technologies, for example) is the most imperative step—it directly addresses the problem of user anonymity that makes hacking, spam, piracy, and identity theft possible. But implementation of interoperable authentication mechanisms and other necessary improvements will require coordinated effort, not just cross-fertilization of ideas. If industry fails to work together voluntarily, government will increasingly step in, creating burdens, not solutions.

Best practices are gradually emerging. Internal procedures like daily data backup are now standard practice, and ISPs and other service providers have assumed responsibility for screening traffic and protecting the backbone hardware. Additionally, companies frequently caution their online customers or users of basic information safety procedures. Safeguards for corporate and other computer networks are also improving. The Internet Security Alliance—a business-led collaboration between members of the Electronic Industries Alliance, and Carnegie Mellon University's Software Engineering Institute and CERT Coordination Center—formed in April 2001. The group addresses risk management, conducts threat assessments, and promotes best practices[70] and publishes a "Top Ten" list of recommended security practices.[71] Internationally, the Organization for Economic Cooperation and Development has taken an interest in cybersecurity, releasing a report in 2002 that included a list of proposed voluntary guidelines.[72]

A sampling of recommendations from these various working groups include: changing software defaults that leave systems open to intruders; hiring more experienced personnel; improving the training of system administrators and network operators; assuring that all new software security patches are installed; improving

firewall, anti-virus and encryption technologies; funding of private security research; employing redundancy in hardware, software, and databases; purchasing insurance against attacks; and hiring independent security companies to remotely monitor corporate networks. Of course the costs of implementing the recommendations and investing in other security measures must be measured against the costs of security breaches.[73] Firms must assess the level of protection they require to determine whether, for example, security checkpoints should exist at multiple levels within a corporate network or just at the perimeter.[74]

In *Information Security Governance: Toward a Framework for Action,* the Business Software Alliance notes that a "remarkable convergence exists...regarding recommended security practices. There is a broad consensus among the experts as to what kinds of measures should be undertaken by organizations."[75] Similarly, some in the legal community have pointed to agreement on broad security principles, recommending the formal "adoption of an intelligently designed and clearly defined security policy, limitation of both internal and external access to sensitive information, and establishment of a disaster recovery plan to be implemented in the event of a security breach."[76] Legal analysts further advise that "individual companies may need to take more stringent measures where the probability of a security breach is particularly high, or the consequences of a breach especially large. And companies should stay aware of technical—as well as legal—developments in the field of information security." [77]

Although the Department of Homeland Security emphasizes security education, the emerging consensus on best practices is not driven by government. Those at risk are increasingly vigilant in defending against physical as well as data attacks. Data centers, the bunker-like facilities housing much of the Internet infrastructure, employ extreme security measures and redundancy techniques, scattering data and equipment spatially across numerous sites and maintaining separate power sources and backup generators to mitigate the effects of full power grid failure on Internet—and information—security.[78] The redundancy and diversification of infrastructure elements, which utilize multiple carriers and multiple backups, are market-inspired innovations. Indeed, according to an *eWeek* report on the state of communications networks after September 11, 2001:

> "[A]bsent a coordinated government infrastructure security policy, private enterprise has managed to evolve its own set of protections. The points at which data and voice traffic are handed off from one network to another are hidden and geographically diverse, and key switching gear is housed in hardened buildings. Redundancies are built into the networks, and the Internet is so widely distributed that it is literally hard to kill."[79]

Although market forces have produced high levels of infrastructure security, there is more to be done across the industry. In his 2002 "Trustworthy Computing" memo to Microsoft employees, Bill Gates identified security—rather than product development—as the company's primary focus, noting that "no trustworthy computing platform exists today."[80] The original elements of the Trustworthy Computing initiative—that software products be secure by design, default (leaving features that expose computers to the outside world turned off until activated by the user), and deployment (making it easier for users to maintain security once up and running)[81]—have evolved into what Scott Charney, Vice President for Trustworthy Computing, calls "a Microsoft corporate tenet that guides nearly everything we do." Charney also notes efforts through the program to generate industry-wide collaboration on security measures.[82] Similarly, Oracle Corporation initiated an "Unbreakable" security campaign.[83] The company's chief security officer called for the software equivalent of Underwriters Laboratories, the product-safety and certification organization: "Thanks to the UL, most consumer products are generally difficult to operate in an insecure fashion. For example, Cuisinarts are designed so that you can't lose a finger while the blades are whirling. We don't expect the consumer to do anything special to operate Cuisinarts securely; they just are secure. Similarly, consumers should not be expected to be rocket scientists or security experts. Industry needs to make it easy to be secure."[84]

Cooperative best security practices evolve in response to market circumstances. Companies like Cisco, Symantec, Trend Macro and Network Associates have teamed up to develop network security solutions in response to consumer demand for better safety.[85] Firms increasingly seek to ensure end-to-end service quality

for highly important applications and priority uses, such as critical communications. But to work, priorities must be communicated over numerous networks, and with secure cooperation among carriers.[86] For example, a teenager's email needn't be assigned the same level of urgency as a stock transaction. Setting the priority level of Internet communications will require not just coordination across networks, but also pricing signals by which information about priorities is relayed to service providers. Government intervention into the Internet to impose network neutrality—the idea that all content and communications should be treated equally—will distort these price signals and lead to economically inefficient prioritization.

Just as companies adapted to automation in physical processes, they are adapting to automate and normalize security processes as well; hardware and software updates are increasingly made as a matter of course. Over the past decades, information technology has automated numerous manual processes, like accounts receivable, inventory management, and tracking of shipments. Now, processes to improve and update information technology itself are being automated.[87]

If coordination and internal practices alone are unable to defend against emerging threats, an entire security industry has emerged that can help. External network monitoring by independent, managed security services are one of today's major responses to cyber-threats; the complexity of keeping up with the latest viruses and patches is an unmanageable feat for many companies.[88] Those that wish to turn over security responsibility completely to an outside firm farm out the job to firms like Genuity, Counterpane, and others. Symantec alone, for example, monitors over 600 company networks. Some companies prefer, however, to keep security an in-house function, perhaps unable to afford comprehensive monitoring, or unconvinced of the quality and trustworthiness of outside vendors.[89] They might prefer security intelligence services that do not entirely assume the security monitoring role, but instead monitor security developments overall and pass intelligence along to in-house technicians.[90]

Raising the Costs of Cluelessness for Individual Users

Not all Internet threats are attributable to product or service shortcomings. Individuals can leave their home PCs—or company networks—open to attack simply through carelessness or ignorance of basic security practices. As mentioned above, companies fill correspondence to both their employees and consumers with warnings about basic security procedures: don't open email attachments from strangers, and be careful even with email from people you know; use firewall and antivirus software, and keep them updated; use tricky passwords and change them often; be on the lookout for "phishing" and "pharming" scams. To a large extent, the vulnerabilities created by individual users can be overcome through education.

But industry must play a role as well in overcoming the challenges posed by human error, which is unfortunately unavoidable. Software and hardware design must make user error more difficult. Software and hardware, for example, can be designed with default settings that provide maximum security with mechanisms to automatically update and upgrade when connected to the Internet. ISPs can take a greater role in monitoring user activity (within the confines of an appropriate privacy policy), creating members-only networks, and advancing the use of biometrics for user authentication.

One interesting development regarding fitness for online participation has been driven by colleges and universities, who, in response to rampaging viruses, cut students' Internet access until their machines are certified and updated.[91] For example, at Oberlin College, students with virus-infected machines are disconnected from the university network. The school also threatens a $25 fine for students spreading a virus to others, even inadvertently.[92] There is no reason other major networks—or even ISPs—couldn't make similar demands of network participants, requiring automatic software patching, relinquishing anonymity, and other restrictions.

As one system administrator colorfully put it, unless people get a "basic working knowledge…techies need to be protected from the clueless."[93] Requirements on users could mean that the problem of ignorant or careless users with poor security habits is a transitory one. Skeptics rightly point out that certifying and policing users with "digital patrol cars" and imposing necessary sanctions is a complex proposition.[94] Nonetheless, behind

calls for individual licensing and user certification is the tacit recognition that it isn't necessarily software and service providers that bear all the blame—yet another reason why government regulation of the industry won't solve the cybersecurity problem. If anything, regulation will divert resources from efforts to better educate individuals and give the impression that users are blameless, no matter how bad their security habits.

The Regulatory Reality: Disincentives Matter Too

Defining Standards Down

Blights like cyber-crime, cyber-nuisance, and identity theft are rampant. Who should play the dominant role in addressing these cybersecurity threats as they emerge? Private sector actors who have a vested interest in protecting their products, reputation, and finances, or government, which unfailingly imposes regulations that stifle innovation and burden businesses, while simultaneously failing at the stated objective? Government responses to problems that are clearly outside of government's control are simply attempts to demonstrate that *something is being done*, with little interest paid to whether it's the *right* thing.

Market incentives for breach disclosure are growing, a superior alternative regulatory requirements.

As the recent Congressional debate over net neutrality indicates, when it comes to technology, lawmakers often understand neither the nature of the problems and the forms they might take nor the repercussions of the proposed solutions.[95] A government stamp of approval for technology can have only two results: the standardization of mediocrity across an entire industry and the guarantee of inefficient allocation of resources. Certain homeland security programs, for example, indemnify makers of government-approved security technologies from liability when they fail. To return to a question asked previously: What happens when the government-approved firewall fails? When neither the regulators who approve the technology nor the businesses that create the technology are held liable, incentives to keep quality high and technology advancing become grossly distorted.

Some public-private information sharing and disclosure make eminent sense, particularly when national security concerns are at stake. But a critical issue in cybersecurity is knowing when to keep information private. Automatic confession of every data breach or potentially exploitable software hole without regard to severity is not a prerequisite for information security. While some information will be valuable if publicized, other information will either become simply white noise to business decision makers, prove unnecessarily damaging to the victimized company, or actually help hackers and other cyber-criminals. For example, the Code Red worm appeared shortly after the vulnerability that made the virus possible was posted online.[96] The Slammer worm appeared several months after the underlying vulnerability was posted by a researcher.

Computer industry players continually debate whether or not it is a good idea to publish code capable of exploiting a security weakness. Although doing so may help system administrators and the developers of the flawed code, the costs and benefits of disclosure vary from case to case. Cybersecurity strategists must carefully study policies regarding disclosures about potentially exploitable software, since such details could themselves be used to mount an attack. There are no universal standards that regulators should cement in place.

Market incentives for breach disclosure are growing, a superior alternative to regulatory requirements. Executives know that the decision *not* to reveal relevant information can hurt a company's market stance if outsiders point out the problem first. It might be best for security monitoring firms to *alert one another behind the scenes* about newfound threats, rather than for their clients to be subject to disclosure requirements. Vibrant market incentives to share what needs sharing but also to downplay false alarms and low-level risks must be allowed to develop. As previously noted, one way to do this is for the industry to fund a third-party

administrator who can alert the developers about vulnerabilities and require a specified time frame for repair. A proposal from the Organization for Internet Safety would give software companies 30 days to patch a flaw before security researchers announce problems.[97]

There are possible roadblocks to the success of a system of third-party monitoring. Announcements by security researchers against the wishes of the software developer may run afoul of the Digital Millennium Copyright Act, a wrinkle that is being explored by Stanford University's Center for Internet and Society.[98] Additionally, some software developers include in their products licensing provisions that prohibit published performance reviews or benchmark/comparison tests without permission. In one instance, a New York court has already called one such ban "deceptive," noting that the software company gave the impression that reviewers would be breaking the law,[99] which can be a gray area. From a contractual standpoint, however, it is entirely appropriate for software vendors to disallow tests, but in doing so, they run the risk of raising questions about the quality of their products among consumers. In today's security-conscious environment, business customers and individual consumers are unlikely to tolerate restrictions on benchmark tests. Participation in the third-party monitoring agreement would demonstrate a cooperative stance and signal product quality, yet another market incentive for openness that regulations can't duplicate. Indeed, regulations requiring full, mandatory self-disclosure invite unscrupulous attempts to downplay problems.

As consumer demand for security increases, audits of private security practices will be driven by insurance and other market forces. Unlike government auditors and monitors who can essentially avoid accountability, private audits will be even more valuable to the extent that auditors themselves are "audited" by the market through ratings firms. Instead of the broad, mandatory disclosures hinted at by Homeland Security, there could be third-party, letter-grade rating systems for cybersecurity. Companies flouting generally agreed-upon security procedures would receive the equivalent of a junk-bond rating for their reputation—or no rating at all.[100] Meanwhile, the firms providing the security ratings would have their own reputations at stake, promoting competition and ever higher standards. Ratings companies would also likely be bound by non-disclosure agreements, overcoming the private sector's discomfort with sharing industry information with government.

This approach—without legislation—would prod the industry away from its perceived secrecy about vulnerabilities and move it toward openness. Furthermore, the emergence of solid rating systems would likely advance hand-in-hand with cyber-insurance: Companies who receive a good rating would qualify for insurance in case an unfortunate attack does succeed. Of course, private rating systems wouldn't be perfect. But by creating the right incentives for compliance—rather than the disincentives for disclosure associated with a one-size fits all solution—a ratings system would be far superior in handling cybersecurity problems than government intervention. Ratings will also have the advantage of being based on responses to problems on a case-by-case basis, unlike the Department of Homeland Security's color code system which sends confusing signals by suggesting that the threat level in Manhattan and the threat level in Topeka are the same.[101]

Political Favor-Seeking

As any student of public policy knows, regulatory agencies can easily form unhealthy relationships with the industries they regulate. Recent scandals highlight the problems that can come from political-favor seeking when key players move seamlessly from lobbying positions to positions of influence in government agencies, and vice versa. Even with worthy intentions, close ties between regulatory bodies and industry can result in policies that are "pro-business" (or, rather, pro-*certain* businesses) but anti-market. For example, common security certifications specified by defense and intelligence agencies can disadvantage small firms who cannot cope with the bureaucratic requirements.[102] In other instances, companies that perform automated audits of corporate networks—a worthwhile task—favor regulation to *require* reporting of such information to the SEC or other federal entity in order to boost their own business. The experts offering policy advice to lawmakers are all too often far from disinterested.

Cybersecurity policy is not immune to favor-seeking practices. A 2003 report from the Computer and Communications Industry Association (CCIA) warned of a software "monoculture," in which the dominance of Windows creates vulnerability by making everyone susceptible to the same flaws.[103] The group wants Microsoft, in the name of security, to allow its programs to interoperate more easily with competitors' software. The Association for Competitive Technology noted, however, that the plan would benefit the CCIA's members at Microsoft's expense, noting, "The study ignores the benefits of homogeneous networks, such as ease of security management and lower security training costs, which offset the potential dangers."[104]

There is merit to the notion of diversity in biology; organisms with some diversity in their makeup can better withstand environmental stresses. While there is an analogy to be made between biological organisms and computer attacks, it is the public character of the Net rather than the brand of software that is the real culprit. The more important feature shared among most attacks is that they originate from anonymous miscreants using the public, open Internet, not that they are launched against a particular, popular type of software. Moreover, there are so many possible configurations of computers running Windows software, and so many forms of virus protection available, that the monoculture analogy to biology is tenuous at best.[105] The monoculture at issue isn't Windows, but ones-and-zeros software itself. (Until quantum, optical, or DNA computing come along, it is a debate that will continue.)

The CCIA case is just one prominent example of how political favor-seeking already occurs. Other examples in cybersecurity could include regulations or licensing fees that would erect barriers to entry and protect the market share of existing market players. Favor-seeking is unavoidable in regulated industries: Industry lobbyists, committee staff, and agency personnel become interdependent on one another, and the outcome is almost never good news for would-be market entrants or consumers. And as regulation increases, the opportunities for manipulation of the regulatory apparatus increase as well.

Technological Lock-In

As discussed above, a lobbyist/appropriations environment in cybersecurity might essentially create a government-imposed oligopoly in the hardware and software market that favors a few select businesses rather than a real marketplace. Government-mandated technology would lock in standards—by locking out competitors—which could undermine research and innovation in the field of secure applications. Some private network security monitoring companies, for instance, rightly opposed White House consideration of a requirement that ISPs develop a "central monitoring system" to monitor the Internet for questionable activity.[106] It is better that ISPs develop such systems independently, so that competition can identify the best technologies.

Following the September 11, 2001 attacks, Oracle CEO Larry Ellison sought to provide software for a national ID card. This proposal flew in the face of the conventional wisdom against locking in technologies, and, had it been accepted, would have increased the likelihood that a single government national ID would displace superior private ones.[107] The last thing government needs to do in the age of identity theft is to give Americans more documents bearing sensitive identifying information; it has already created a needless identity theft problem with the Social Security number and its widespread—and inappropriate—use as identification.

Online piracy, another issue bearing some relationship to cybersecurity problems, also raises concerns over the appropriateness of technological standards set by government. Some proposals would mandate copy-protection technologies to prevent piracy.[108] These so-called "digital rights management" techniques are perfectly appropriate, even necessary, for intellectual property holders who wish to protect their digital content—like music, movies, electronic books, and digital broadcasts—from unauthorized duplication. The problem arises when inferior technologies are mandated.

It's likely that some advocates of governmental cybersecurity standards oppose government mandates with respect to copy protection. But information security can benefit from private innovation in piracy prevention and digital rights management and vice versa, with no need for government standards in either area. Cross-fertilization will be unpredictable, and too fluid for government to successfully be able to choose among

strategies. Alhough companies are always free to move above a government mandated floor—such as makers of fuel efficient cars who voluntarily exceed government performance standards—a floor can easily become a ceiling for many companies, a bare minimum above which there is no point in going. Incentives to push above the mandated standards are thus hampered.[109] It would be hard to blame a service provider for an attack if he has complied with the law.

Conclusion: Following the "Cybersecurity Commandment"

Policymakers should recognize that data security requires not one-size-fits-all solutions, but the tailored answers that private actors can deliver. Every firm's upstream suppliers and downstream customers increasingly demand better security. Like any other technology, security technologies, from biometric identifiers to firewalls to encrypted databases, benefit from competition. Likewise, cybersecurity services, from consulting to insurance to network monitoring, benefit from competition. To reduce the impact of any given attack, policy makers should adhere to policies that, to the extent possible, "privatize" rather than collectivize.

The need to preserve a dynamic market role can be summed up in a single Cybersecurity Commandment:

> *Do not take steps in the name of security that make it:*
>
> *(1) impossible to liberalize or deregulate infrastructure or*
>
> *(2) impossible or undesirable to self-regulate*.

Government should not assert authority in ways that would make private sector assumption of security responsibility impossible in the future as technology advances or conditions change. And policy makers should be extremely careful not to create *disincentives* to self-regulation. If government ignores either aspect of the Cybersecurity Commandment, it will lead to both subpar information security and economic inefficiencies. Interference could also roll back important advances that have been made in the privatization of infrastructure and services over the past decades.

Government should not assert authority in ways that would make private sector assumption of security responsibility impossible in the future as technology advances or conditions change.

Government power adopted to address a crisis tends to stay in place after the crisis passes, a phenomenon dubbed the "ratchet effect" by economist Robert Higgs.[110] Power to control information security efforts will not be immune to this effect. If recent high-profile identity theft episodes result in regulations that add complexity but not improvement to information security processes, government will not willingly give up the political power that accompanies the power to regulate, even if technological advances or industry effort make further intervention unnecessary. Under the umbrella of government oversight, just about anything electronic and networked could fall under the rubric of cybersecurity regulation. It doesn't take much imagination to see how the ratchet effect will deleteriously undermine the security and robustness of critical infrastructures, basic Internet operations, and technological progress. In the final analysis, it is the private sector that occupies the only territory from which a successful defense against attacks on hardware and information can be mounted.

Notes

[1] Reuters, "Symantec CEO Warns of Regulation Over IT Security," November 19, 2003. http://www.bizreport.com/article.php?art_id=5578.
[2] Robert Lemos, "Congress May Tighten Web Security," *CNET News.com*, November 7, 2001. http://news.com.com/2100-1001-275550.html?tag=rn.
[3] Brian Krebs, "Congressman Puts Cybersecurity Plan On Hold," *washingtonpost.com*, November 4, 2003. http://www.washingtonpost.com/ac2/wp-dyn/A63587-2003Nov4?language=printer.
[4] Quoted in Robert Lemos, "Government Unveils Cybersecurity Plan," *Cnet News.com*, September 18, 2002. http://news.com.com/2100-1023-956353.html.
[5] Alan Charles Raul, Frank R. Volpe and Gabriel S. Meyer, Liability for Computer Glitches and Online Security Lapses, Washington, D.C. office of Sidley Austin Brown & Wood, August 2001. http://www.sidley.com/cyberlaw/features/liability.asp.
[6] http://www.whitehouse.gov/pcipb/.
[7] See Robert Lemos and Declan McCullagh, "Cybersecurity Plan Lacks Muscle," *News.com*, September 19, 2002. http://news.com.com/2102-1023-958545.html.
[8] George Smith, "A Cybersecurity Sleeping Pill," *SecurityFocus Online*, September 23, 2002. http://online.securityfocus.com/columnists/110.
[9] Kevin Poulsen, "Cybersecurity Plan Offends No One," *SecurityFocus Online*, September 18, 2002. http://online.securityfocus.com/news/677.
[10] Bruce Schneier, "National Strategy to Secure Cyberspace," *Crypto-Gram Newsletter*, October 15, 2002. http://www.counterpane.com/crypto-gram-0210.html.
[11] Fred Avolio, "Securing Cyberspace—Comments On the National Strategy, *NetSec Letter #21*, October 2, 2002 http://www.avolio.com/columns/21-SecuringCyberspace.HTML.
[12] Gary Warner, *Input to the National Strategy to Secure CyberSpace on Behalf of the Membership of FBI InfraGard* 2002. http://www.infragard.net/library/national_strategy.pdf.
[13] Cited in Brian Krebs, "Cybersecurity Deadline Looms, Release Date Remains Hazy, "*washingtonpost.com*. November 18, 2002. http://www.washingtonpost.com/ac2/wp-dyn/A6152-2002Nov18.
[14] Ranum 2002.
[15] *The National Strategy to Secure Cyberspace*, The White House, February 2003. p. ix. http://www.whitehouse.gov/pcipb/executive_summary.pdf.
[16] *The National Strategy to Secure Cyberspace* (Draft for Comment), The President's Critical Infrastructure Protection Board, The White House, September 2002. p. 8. http://www.isalliance.org/resources/papers/NationalStrategy9.18.02.pdf.
[17] Ibid, Krim, December 4, 2003.
[18] See, "Statement of Senator Feinstein on New Details of Major Data Breach," (posted on Senator's website: http://feinstein.senate.gov/05releases/r-idtheft-lexis3.htm) April 12, 2005.
[19] Richard H. Levey, "Data Bills Pile Up in Congress," *DirectNews Online*, October 15, 2005. http://www.directmag.com/mag/marketing_data_bills_pile/.
[20] United States Congress, House of Representatives: 109th Congress, 1st Session. H.R. 4127, A bill to protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach [introduced in the U.S. House of Representatives, October 25, 2005]. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4127ih.txt.pdf.
[21] Ibid, Amendment to H.R. 4127, as Reported by the Subcommittee.
[22] United States Congress, Senate: 109th Congress, 1st Session. S. 1789, A bill To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information [introduced in the U.S. Senate, September 29, 2005 and reported with an amendment, November 17, 2005]. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1789rs.txt.pdf
[23] Declan McCullagh, "Preliminary Analysis of New Specter-Leahy Data Security Bill," *PoliTech: Politics and Technology*, June 30, 2005. http://www.politechbot.com/2005/06/30/preliminary-analysis-of/
[24] Amy Harmon, "Digital Vandalism Spurs a Call for Oversight," *The New York Times*, September 1, 2003. p. A1.
[25] Peter R. Orszag, Joseph A. Pechman Senior Fellow in Economic Studies, The Brookings Institution. *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives*.
Testimony before the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security, House Select Committee on Homeland Security, September 4, 2003. http://www.iwar.org.uk/cip/resources/energy/orszag090403,.pdf.
[26] Bruce Schneier, "National Strategy to Secure Cyberspace," *CRYPTO-GRAM*, October 15, 2002.
[27] Orszag, p. 3.
[28] Fred E. Foldvary and Daniel B. Klein, editors, *The Half-Life of Policy Rationales*, New York University Press: New York. 2003.
[29] Marcus J. Ranum, "Federal Cybersecurity: Get a Backbone," *TISC Insight*, Volume 4, Issue 14. http://www.tisc2002.com/newsletters/414.html.
[30] Grant Gross, "Congress Looks for Cybersecurity Answers," *InfoWorld*, September 10, 2003. http://www.infoworld.com/

article/03/09/10/Hncongresscyber_1.html?security.
[31] Noted in Patrick Ross, "Limited Cybersecurity Role Seen for Federal Government," *Washington Internet Daily*, Vol. 4, No. 224, November 20, 2003. p. 1-2.
[32] See Steve Peacock, "Bill to Hold Chief Information Officers Accountable for Security Seen," *Washington Internet Daily*, October 30, 2002. p. 2.
[33] Neil Munro, "Cybersecurity Regulations Imminent, Industry and Government Warn," *GovExec.com*, September 30, 2002. http://www.govexec.com/dailyfed/0902/093002nj.htm.
[34] For an overview see Clyde Wayne Crews Jr., "Cybersecurity and Authentication: the Marketplace Role in Rethinking Anonymity—Before Regulators Intervene," *Competitive Enterprise Institute Issue Analysis 2004 No. 2*, November 8, 2004. http://www.cei.org/pdf/4281.pdf.
[35] Dropped proposals noted in D. Ian Hopper and Ted Bridis, "Parts of Cybersecurity Plan Removed," Associated Press, September 17, 2002. http://www.cbsnews.com/stories/2002/09/18/tech/main522419.shtml.
[36] Robert Lemos, "Bush Unveils Final Cybersecurity Plan," *CNET News.com*, February 14, 2003. http://news.com.com/2100-1001-984697.html.
[37] "NAIC Decides Against Mandatory Cybersecurity Testing," *Washington Internet Daily*, January 9, 2003. p. 3.
[38] Lemos and McCullagh, September 19, 2002.
[39] Noted in Declan McCullagh, "Homeland Defense Focus Shifts to Tech," *CNET News.com*, July 10, 2002. http://news.com.com/2100-1023-942686.html?tag=prntfr.
[40] Reported in Associated Press, "Execs Try to Slow Tech Security Rules," *CNN.com*, December 3, 2003. http://us.cnn.com/2003/TECH/biztech/12/03/computer.security.ap/.
41 See Grant Gross, "Congress Takes Small Steps On Privacy Legislation" *InfoWorld*, July 18, 2003. http://www.infoworld.com/article/03/07/18/HNsmallsteps_1.html.
[42] Ted Bridis, "Bill Would Require Companies to Notify Customers When Accounts Are Hacked," Associated Press, June 27, 2003. http://www.securityfocus.com/news/6184.
[43] Chris Gaither, ""Law Requires That Firms Reveal Security Breaches," *The Boston Globe*, June 23, 2003. p. C1. See also Rachel Konrad, "U.S. Law to Warn of Identity Theft," *Australian IT*, June 23, 2003. http://australianit.news.com.au/articles/0,7204,6638912%5e15319%5e%5enbv%5e15306,00.html.
[44] Farhad Manjoo, "So Many Worms, So Little Info," *Wired News*, April 10, 2001. http://www.wired.com/news/print/0,1294,42945,00.html.
[45] Caroline E. Mayer, "Plan Would Ask Banks to Warn of Data Vulnerability," *The Washington Post*, August 13, 2003. p. E5. http://www.washingtonpost.com/wp-dyn/articles/A51690-2003Aug12.html.
[46] See Caroline E. Mayer, "Guidelines Aim to Help Prevent ID theft," *The Age*, August 19, 2003. http://www.theage.com.au/articles/2003/08/18/1061059762804.html?from=storyrhs.
[47] Robert Vamosi, "My Plan for Fixing Software Flaws," *ZDNet.com*, October 2, 2002. http://www.zdnet.com/anchordesk/stories/story/0,10738,2882094,00.html.
[48] possible citation? http://www.usatoday.com/tech/news/computersecurity/2003-10-09-sec-cyberfiling-idea_x.htm
[49] Patrick Ross, "Former NIPC Chief Calls for 'Soft' Cybersecurity Regulation," *Washington Internet Daily*, April 9, 2003. p. 2.
[50] Ibid. Ross, April 9, 2003.
[51] Ibid, Harmon, 2003.
[52] Grant Gross, "Congress Looks for Cybersecurity Answers," *InfoWorld*, September 10, 2003, http://www.infoworld.com/article/03/09/10/Hncongresscyber_1.html?security.
[53] Ted Leventhal, "Panel Chairman Will Push for a Cybersecurity Mandate," *National Journal's Technology Daily*, July 10, 2003. See also Andrew Goodman, "Public Must Trust Information Security to Do E-Government, Forum Says," *Washington Internet Daily*, July 11, 2003. p 3-5.
[54] Brian Krebs, "Congressman Puts Cybersecurity Plan On Hold," *washingtonpost.com*, November 4, 2003. http://www.washingtonpost.com/ac2/wp-dyn/A63587-2003Nov4?language=printer.
[55] The Homeland Security Advisory System is located at http://www.dhs.gov/dhspublic/display?theme=29.
[56] Clyde Wayne Crews Jr., "Cybersecurity Finger-pointing: Regulation vs. Markets for Software Liability, Information Security, and Insurance," *Competitive Enterprise Institute Issue Analysis 2005 No. 6*, May 31, 2005. http://www.cei.org/pdf/4569.pdf.
[57] Michael Bartlett, "ICANN: U.S. Official Says Government Should Stay Out of Internet," *Newsbytes.com*, November 14, 2001. http://www.findarticles.com/cf_dls/m0NEW/2001_Nov_14/80093148/p1/article.jhtml. Note: The Critical Infrastructure Assurance Office has been incorporated into the Department of Homeland Security under the Information Analysis and Infrastructure Protection Directorate.
[58] See Brian Krebs, "Online Financial Crime Headed From Bad to Worse," *washingtonpost.com*, December 17, 2003. http://www.washingtonpost.com/ac2/wp-dyn/A5934-2003Dec16?language=printer.
[59] Peter Fishburn, Andrew M. Odlyzko, and Ryan C. Siders, "Fixed fees versus unit pricing for information goods: competition, equilibria, and price wars," First Monday (Peer Reviewed Journal on the Internet), 1996. http://www.firstmonday.dk/issues/issue2_7/odlyzko/
[60] Larry Seltzer, "Throw Away the Internet; Start All Over," *Ziff Davis Security Supersite*, April 21, 2003. http://www.eweek.com/article2/0,1759,1241632,00.asp.

[61] Will Knight, "Puzzles Could Block Mass Computer Attacks," *NewScientist.com*, May 14, 2003. http://www.newscientist.com/news/print.jsp?id=ns99993729.
[62] Kevin Newcomb, "AOL to Implement Certified E-mail Program," *ClickZ News*, January 30, 2006. http://www.clickz.com/news/article.php/3581301
[63] See, for example, Dear AOL's "Open Letter to AOL" at www.dearaol.com, February 28, 2006.
[64] Pamela Parker, "California Lawmaker to Hold Hearings on AOL Email Plan," *ClickZ News*, March 15, 2005. http://www.clickz.com/news/article.php/3591626
[65] Christopher Wysopal, Director of Research and Development, @stake, Inc., *Testimony for the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Hearing on "Worm and Virus Defense: How Can We Protect the Nation's Computers from These Threats?*" September, 2003. http://www.atstake.com/events_news/wysopal_testimony.pdf.
[66] Testimony of Richard D. Pethia, Director, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Before the House Committee on Government Reform,
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census,
Hearing on Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats? September 10, 2003.
http://www.cert.org/congressional_testimony/Pethia-Testimony-9-10-2003.
[67] See Susan Polyakova, "FCC's TAC Calls Network Vulnerability Major Issue in VoIP Growth," *Washington Internet Daily*, Vol. 4, No. 203. October 21, 2003.
[68] Arnold Kling, "Security Intervention?" *TechCentralStation*, October 1, 2003.
http://www.techcentralstation.com/100103D.html.
[69] Fred L. Smith Jr., "Cowboys Versus Cattle Thieves: The Role of Innovative Institutions In Managing Risks Along the Frontier," in Christopher L. Culp and William A. Niskanen, editors, *Corporate Aftershock: The Public Policy Lessons From the Collapse of Enron and Other Major Corporations*, John Wiley & Sons: Hoboken, New Jersey, 2003. p. 275.
[70] Press Release, "Internet Security Alliance Launched," Internet Security Alliance, April 19, 2001. http://www.sei.cmu.edu/about/press/isalaunch_release.html.
[71] Internet Security Alliance*, Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices*, July 2002. http://www.isalliance.org/news/BestPractices.pdf.
[72]Sandeep Junnarkar, "Group Promotes 'Culture of Security'" *CNET News.com*, August 26, 2002. http://news.com.com/2100-1001-955307.html. Report available at http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)6-final.
[73] Internet Security Alliance, *Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices*, July 2002. p. 4.
[74] Ibid, http://zdnet.com.com/2102-1105-829686.html.
[75] Ibid. *Information Security Governance: Toward a Framework for Action*: White paper, October 2003. http://www.globaltechsummit.net/press/ISGPaper-2003.pdf.
[76] Alan Charles Raul, Frank R. Volpe and Gabriel S. Meyer, August 2001.
[77] Ibid.
[78] Kenneth Bredmeier and Sarah Schafer, "Data Bunkers Protect Off-Site Sites," *The Washington Post*, November 9, 1999. p. A. 1.
[79] Dana Coffield, "Networks at Risk: Assessing Vulnerabilities," *Interactive Week*, September 24, 2001. p. 14. http://www.pcmag.com/article2/0,1759,158275,00.asp.
[80] Jonathan Krim, "Gates Says Software Security Is a Priority," *The Washingington Post*, p. E1. January 17, 2002.
[81] Testimony of Scott Charney, Chief Trustworthy Computing Strategist, Microsoft Corporation, "Cybersecurity & Consumer Data: What's at Risk for the Consumer?" Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce, November 19, 2003. http://energycommerce.house.gov/108/Hearings/11192003hearing1133/Charney1794print.htm.
[82] Scott Charney, "Momentum and Commitment: Trustworthy Computing After Four Years," February 8, 2006, http://www.microsoft.com/mscorp/twc/2005review.mspx.
[83] See Alex Salkever, "Backing Up Oracle's 'Unbreakable' Vow," *BusinessWeek Online*, January 15, 2002. http://www.businessweek.com/bwdaily/dnflash/jan2002/nf20020115_8894.htm.
[84] Ms. Mary Ann Davidson, Chief Security Officer, Oracle Corporation,"Cybersecurity & Consumer Data: What's at Risk for the Consumer?" Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce, November 19, 2003. http://energycommerce.house.gov/108/Hearings/11192003hearing1133/Davidson1796print.htm.
[85] Erika Morphy, "Cisco's Gang of Four Tackles Security Fears, *NewsFactor*, November 19, 2003. http://story.news.yahoo.com/news?tmpl=story&u=/nf/20031119/tc_nf/22725.
[86] Rowan Winters, "Internet 2," *ComputerSource*, July, 1999. Available at http://www.sourcemagazine.com/archive/799/feature3.asp. **[check link]**
[87] See David Kirkpatrick, "Taking Back the Net," *Fortune*, September 29, 2003. p. 120. http://elab.vanderbilt.edu/infokit/FORTUNE%20092903.pdf.
[88] See John Schwartz, "Last Boom In Town: Demand Still Grows for Online Security," *New York Times*, April 18, 2001. p. 13. http://www.nytimes.com/2001/04/18/technology/18SCHW.html.
[89] George V. Hulme, "Security's Best Friend?" *Informationweek.com*, July 16, 2001, pp. 38-44. http://www.informationweek.com/story/IWK20010713S0009.
[90] Brian Ploskina, "Net Vigilance," *Interactive Week*, July 17, 2001. http://www.zdnet.com.au/newstech/security/story/0,2000024985,

20241014,00.htm.
[91] Brian Krebs, "Universities Rush to Protect Networks," *washingtonpost.com*, September 4, 2003. http://www.washingtonpost.com/ac2/wp-dyn/A25845-2003Sep4?language=printer.
[92] Associated Press, "Colleges Crack Down on Viruses," *Wired News*, September 4, 2003. http://www.wired.com/news/technology/0,1282,60299,00.html.
[93] Michelle Delio, "License PC Users? It's a Thought," *Wired* News, August 16, 2001. http://www.wired.com/news/politics/0,1283,46096,00.html.
[94] Michelle Delio, "License PC Users? It's a Thought," *Wired* News, August 16, 2001. http://www.wired.com/news/politics/0,1283,46096,00.html.
[95] Anne Broache, "Democrats Attack New Bill Over Net Neutrality," *CNET News.com*, March 30, 2006. http://marketwatch-cnet.com.com /2100-1036_3-6056156.html
[96] Noted in Testimony of C. Warren Axelrod, Director, Global Information Security, Pershing, Cyber Security: "Private-Sector Efforts Addressing Cyber Threats," House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, November 15, 2001. http://energycommerce.house.gov/107/hearings/11152001Hearing420/Axelrod723.htm.
[97] Robert Lemos, "Panel Defends Flaw Disclosure Guidelines," *CNET News.com*, July 30, 2003. http://news.com.com/2100-1002_3-5057914.html?tag=prntfr.
[98] Noted in Declan McCullagh, "Hackers Get Lesson In the Law," *CNET News.com*, August 1, 2003. http://news.com.com/2100-1009-5058918.html.
[99] Lisa M. Bowman, "Court: Network Associates Can't Gag Users," *CNET News.com*, January 17, 2003. http://news.com.com/2100-1023-981228.html.
[100] Mark Rasch, "This Firm Is Not Yet Rated," *Wired*, January 2004. p. 64-65. http://www.wired.com/wired/archive/12.01/view.html?pg=1.
[101] Charles V. Peña, "Back to Yellow Alert -- But What Changed?" *Cato Commentary*, September 25, 2002, http://www.cato.org/dailys/09-25-02-2.html. See also Charles V. Peña, "Homeland Security: Follow the Bouncing Ball," *Cato Commentary*, May 6, 2003, http://www.cato.org/dailys/05-06-03.html
[102] Noted in Terry Lane, "Putnam Investigates Cybersecurity Criteria for Software," *Washington Internet Daily*, September 18, 2003. p. 3.
[103] *Cyber*In*security: The Cost of Monopoly: How the Dominance of Microsoft's Products Poses a Risk to Security*. White Paper, Computer and Communications Industry Association. September 2003. http://www.ccianet.org/papers/cyberinsecurity.pdf.
[104] Noted in Louis Trager, "MS, Allies Reject Policy Aims of Security Critics of Windows Dominance," *Washington Internet Daily*, September 26, 2003, p. 5.
[105] Marcus J. Ranum, "The Myth of Monoculture," October 13, 2003. http://www.ranum.com/security/computer_security/.
[106] Bara Vaida and William New, "National Cybersecurity Plan Omits Industry Mandates," *National Journal's Technology Daily*, January 6, 2003.
[107] For one discussion of this notion, see Clyde Wayne Crews Jr, Human Bar Code: Monitoring Biometric Technologies in a Free Society, *Cato Policy Analysis No. 452*, September 17, 2002, http://www.cato.org/pubs/pas/pa452.pdf.
[108] For an overview of the debate over government intervention in digital rights management technologiees, see the section on the Security Systems Standards and Certification Act in Wayne Crews and Adam Thierer, "The Digital Dirty Dozen: The Most Destructive High-Tech Legislative Measures of the 107th Congress," *Cato Institute Policy Analysis*, No. 423 February 4, 2002. http://www.cato.org/pubs/pas/pa423.pdf.
[109] One view is that of Larry Clinton, Executive Director of the Internet Security Alliance: "A floor becomes a ceiling…There's very little incentive to push above the floor." Cited in Patrick Ross, "Cybersecurity Companies Urge Congress to Avoid Regulation," *Washington Internet Daily*, February 11, 2003. p. 3.
[110] See Robert Higgs, *Crisis and Leviathan: Critical Episodes in the Growth of American Government*, Oxford University Press, March 1989.

About the Authors

Clyde Wayne Crews, Jr. is Vice President for Policy and Director of Technology Studies at the Competitive Enterprise Institute. His work includes regulatory reform, antitrust and competition policy, safety and environmental issues, and various information-age concerns such as e-commerce, privacy, "spam," broadband, and intellectual property. He is the author of the annual report, *Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State*. Crews is co-editor of the books *Who Rules the Net: Internet Governance and Jurisdiction* (2003) and C*opy Fights: The Future of Intellectual Property In the Information Age* (2002). He is co-author of *What's Yours Is Mine: Open Access and the Rise of Infrastructure Socialism* (2003), and a contributing author to others.

Crews has published in outlets such as the *Wall Street Journal*, *Chicago Tribune*, *Forbes*, *Atlanta Journal-Constitution*, *Communications Lawyer*, and the *Electricity Journal*. He has made various TV appearances on Fox, CNN, ABC and others, and his regulatory reform ideas have been featured prominently in such publications as the *Washington Post*, *Forbes* and *Investor's Business Daily*. He is frequently invited to speak, and has testified before several congressional committees.

Brooke Oberwetter is a policy analyst at the Competitive Enterprise Institute, where she researches and writes on a range of regulatory issues, from FDA regulation, internet, content, and privacy regulation, environmental policy, and attorney general activism. Her specific research interests are the "nanny-state" issues, including the war on obesity, tobacco and alcohol regulation, and consumer protection measures.

Prior to joining CEI, Brooke was a research assistant at the Cato Institute, where she worked on both Social Security and welfare reform. Her writing has appeared in Reason online, the American Spectator online, National Review Online, and other publications. Brooke is also a member of the board of directors of America's Future Foundation and former director of the now-defunct Ban-the-Ban, an ill-fated grassroots organization opposing the passage of a smoking ban in Washington, DC.

$8.00

The Competitive Enterprise Institute is a non-profit public policy organization dedicated to the principles of free enterprise and limited government. We believe that consumers are best helped not by government regulation but by being allowed to make their own choices in a free marketplace. Since its founding in 1984, CEI has grown into an influential Washington institution.

We are nationally recognized as a leading voice on a broad range of regulatory issues ranging from environmental laws to antitrust policy to regulatory risk. CEI is not a traditional "think tank." We frequently produce groundbreaking research on regulatory issues, but our work does not stop there. It is not enough to simply identify and articulate solutions to public policy problems; it is also necessary to defend and promote those solutions. For that reason, we are actively engaged in many phases of the public policy debate.

We reach out to the public and the media to ensure that our ideas are heard, work with policymakers to ensure that they are implemented and, when necessary, take our arguments to court to ensure the law is upheld. This "full service approach" to public policy makes us an effective and powerful force for economic freedom.

Competitive
Enterprise
Institute

1001 Connecticut Avenue, NW
Suite 1250
Washington, DC 20036
202-331-1010
Fax 202-331-0640
www.cei.org

Issue Analysis is a series of policy studies published by the Competitive Enterprise Institute. Nothing in *Issue Analysis* should be construed as necessarily reflecting the views of CEI or as an attempt to aid or hinder the passage of any bill before Congress. Contact CEI for reprint permission. Additional copies of *Issue Analysis* may be purchased through CEI's publications department (pubs@cei.org or 202-331-1010).