POLICY *Review*

FEBRUARY & MARCH 2012, NO. 171

State-level Cybersecurity

By MICHAEL J. GLENNON

State-level Cybersecurity

By Michael J. Glennon

The parade of horribles potentially set to march by a cyberattack is by now familiar: No air traffic controllers or airport check-ins; no electronically regulated rail traffic; no computer-dependent overnight deliveries of packages or mail; no paychecks for millions of workers whose employers depend on payroll software; no financial records of funds on deposit and no ATMs; no reliable digital records in hospitals and health centers; no electrical power, resulting in no light, no heat, no operating oil refineries or heating fuel or gasoline; no traffic signals, and no telephone or internet service or effective police protection — such is the list of what could be disabled by an attack on America's computer networks.

Addressing this threat has been assumed to be the task of the federal government. But the dangers posed clearly implicate the police powers traditionally exercised by the states — and the states' interests are significant. As the authors of one recent study noted, states hold the most comprehensive collection of personally identifiable information about their residents, and

---

Michael J. Glennon is professor of International Law at the Fletcher School of Law & Diplomacy, Tufts University. *This article was supported by a grant from the Hitachi Foundation and is adapted from his book,* Foreign Affairs Federalism, *which will be published by Oxford University Press. The author thanks Matthew Hoisington for research assistance.*

states routinely rely upon the internet to serve those residents. Health and driving records, educational and criminal records, professional licenses and tax information all are held by state governments.

What role, then, might states play in promoting cybersecurity? Just how great is the threat from cyberattacks? What, indeed, is a cyberattack? How effective are federal and international safeguards? Isn't cybersecurity the proper domain of federal law and international law, rather than the states?

Let's begin with the gravity of the threat. So far as we are aware, as James Lewis has pointed out, in only two incidents have actions taken in cyberspace thus far caused serious damage to critical infrastructure. Neither occurred in the United States. (The first involved the disruption of Syrian air defenses by the Israeli Air Force during the destruction of a Syrian nuclear reactor. The second involved the so-called Stuxnet attacks on Iranian nuclear reactors.) These operations were appropriately termed cyberattacks. They involved destruction or disruption of the sort associated with war; they are thus regulated — to a point — by the international law of armed conflict. Cyber-espionage, on the other hand, involves no destruction or disruption but is aimed at the surreptitious extraction of data. The term cybercrime has been used broadly to describe a wide range of activities, from illegal interference and illegal access to the misuse of devices and content-related offenses. Each of these terms refers as much to the perpetrators as to the act itself. Espionage conducted by other nations has been regarded as a matter for the federal government, whereas theft, the destruction of property, and related offenses committed by individuals and criminal organizations are thought to be the purview of both state and federal governments.

What role might states play in promoting cybersecurity? Just how great is the threat from cyberattacks?

While these distinctions provide a bit of analytic clarity, cyberattacks, cybercrimes, and cyber-espionage do not fit well into existing categories. For one thing, they're usually not easily distinguishable from one another until well after their initiation, if then. All exploit vulnerabilities in computer networks and use similar techniques. Malware that has been downloaded surreptitiously and sits silently on a computer may be intended simply to monitor keystrokes — or it may await the command of a distant operator to erase data, freeze the operating system, or participate in a botnet attack (explained below). Experts often cannot be sure what's afoot without time-consuming and painstaking forensic analysis. Given the instantaneity of strike and counterstrike in cyberspace, this can be impractical. Further, the anonymity of cyberspace and the current state of information technology make it extremely difficult to identify transgressors and to attribute attacks. The absence of attributability severely complicates the application of any legal regime to individual acts. Finally, as with terrorist attacks, vexing issues

of legal categorization arise. Flying an airplane into a building is an offense dealt with by state criminal law, federal criminal law, and also — if the attack originates from abroad — international law. So too with a cyber-operation that derails a train or zeros out a bank account.

For all these reasons, the term "cyber-intrusions," while simplistic, is a useful catch-all.

The intrusions' spread

All that said and legalist categories aside, there's clear cause for concern. Cyber-intrusions are growing in frequency and severity. The 2009 breach of Google's e-mail accounts was widely reported. Later that year, computer hackers succeeded in penetrating elements of the U.S. electrical grid and implanted malware that could have allowed wrongdoers to take control of at least parts of the system. After PayPal stopped processing donations for WikiLeaks in 2010, groups such as Anonymous, LulzSec, and other WikiLeaks supporters launched a botnet attack on PayPal's website. Visa and MasterCard were also attacked after announcing that they would not do further business with WikiLeaks (more on this later). A 2011 cyber-intrusion into Sony's PlayStation network might have compromised credit card data, e-mail addresses, and other personal information from 77 million user accounts. The names, account numbers, and contact information of 300,000 Citigroup customers were also improperly accessed in 2011. The security firm RSA disclosed in 2011 that information integral to the security of numerous government and corporate computer networks and e-mail systems had also been extracted from its servers.

These intrusions all occurred within the United States, or at least against U.S. targets. Foreign targets have been hit even harder. A 2007 botnet attack on the Estonian government's servers wrought havoc throughout the country. "All major commercial banks, telcos, media outlets, and name servers — the phone books of the internet — felt the impact, and this affected the majority of the Estonian population," the defense minister said. "This was the first time that a botnet threatened the national security of an entire nation." Georgia was the victim of a similar botnet attack in 2008. A debilitating attack occurred in 2011 against a South Korean bank. One of the most significant cyber-intrusions was revealed later that year when an American cybersecurity company reported that it had identified a single perpetrator of cyber-espionage that lasted up to five years against a wide range of governments, American corporations and even United Nations groups, and that the pattern of targets suggested the perpetrator was a government. Numerous other serious incidents have occurred, but publicly available information is incomplete. Victims of cyber-intrusions tend to be tightlipped for fear of spreading panic or exposing vulnerabilities.

The media attention accorded attacks on these big-name targets might lead one to believe that smaller organizations are safer. They are not. As the vice president of MacAfee's threat research division, Dimitri Alperovitch, recently put it, "the only organizations that are exempt from [cyber-intrusions] are those that don't have anything valuable or interesting worth stealing." Smaller businesses and low-level governmental entities have fewer protections in place and represent low-hanging fruit. Cyber-intrusions against such websites have provided a treasure trove of sensitive information. In August 2011, Anonymous revealed that it had accessed over 70 mostly local law enforcement websites in the United States in retaliation for the arrests of its supporters. The information included names and reports of police tipsters, profiles of gang members, data about security training, and credit card numbers. Some county sheriffs were unaware that their websites had been hacked until they were contacted by journalists.

Anonymous publicly took credit for these intrusions. Normally, however, identifying the source of an intrusion is extremely difficult. Sophisticated cyber-intrusions of the sort launched by governments are especially difficult to trace. Intrusions that don't originate from a given country can be made to appear as though they do, simply by planting a "false flag" in the virus's code. Even if the keyboard from which the intrusion originated can be identified, linking a perpetrator to that keyboard can be impossible (as is linking the perpetrator, if identified, to a government or other organization). Nonetheless, although many such intrusions might have been routed through the United States, what is significant for purposes of considering states' cybersecurity powers is that many do originate abroad, particularly from China.

That being the case, one might, quite logically, look first to international law for protection.

The shortcomings of international law

Alas, international law does little to thwart cyber-intrusions. For several reasons, that is not likely to change. First, it's not clear that traditional rules limiting use of force are relevant to even the most severe form of cyber-intrusions — cyberattacks that are intended to cause destruction and harm. The United States and its allies have long argued that the current rules limit only "armed" attack — violence involving "kinetic" weaponry, not cutoffs of foreign aid, trade boycotts, travel bans, or other acts that might have the same effects as an armed attack. That interpretation is now widely accepted. Few will be persuaded if the United States and its newly vulnerable allies now reverse course and contend that it's really an attack's effects that count, not the means.

Second, it's doubtful that new international legal rules on cyberattacks are possible. Compliance with an international agreement probably could not be

verified, since verification requires the ability to identify transgressors. Some analysts hope that customary norms will emerge from *ad hoc* state practice, as they did long ago concerning diplomatic immunity and freedom of the seas. But that's not likely. Nations' cyber-behavior is veiled in secrecy, which makes it extremely difficult, if not impossible, to find any dots to connect.

Third, even if international rules can somehow be agreed to, it's doubtful they would be effective. Recall, again, Stuxnet. The author of the Stuxnet virus that hamstrung the computer systems running Iran's nuclear centrifuges has never been positively identified (though signs point to the United States and Israel). Some argue that this sort of cyberattack on a country's critical infrastructure should be off-limits. Yet it's hard to see how a ban could have any teeth. When no one knows whether rules are being honored, violators face no penalty and have no incentive to comply. The sole treaty that addresses the issue of cyber-intrusions, the Convention on Cybercrime, discussed later, provides a framework for law enforcement, but its provisions have proven notoriously ineffective as nations have struggled to find the common ground necessary to keep pace with evolving threats. Moreover, the Convention does nothing to address what many commentators see as the brunt of the problem — cyber-intrusions conducted by nations themselves.

The Convention on Cybercrime provides a framework for law enforcement, but its provisions have proven ineffective.

Fourth, it's debatable whether effective international legal limits are desirable. Despite the controversy surrounding Stuxnet, its benefits were significant. It risked none of the casualties that air strikes could have entailed. It might have been more effective. It was probably cheaper. Retaliation was less likely because the attack was anonymized. The use of a cyber-weapon might have averted full-scale war. Some propose holding states accountable for cyber-intrusions that come from within their territory, but the attribution problem would still loom large — and "strict liability" could easily boomerang; many cyber-intrusions, again, originate within the United States.

International limits on cyber-intrusions are therefore likely to remain elusive. The central obstacle to legal restraints is the internet's opaqueness, which allows attackers to disguise their identities and mask the source of the attack. Given the original design of the internet, it's unlikely that nations will succeed in piercing that opaqueness through technological innovation. Absent an ability to attribute responsibility for cyber-intrusions, the best defense will therefore continue to lie not in international law but in national efforts to defend against them and mitigate their effects.

This is where the states can play a pivotal role. They can take firm steps to prevent cyber-intrusions, monitor malicious traffic, mandate cybersecurity measures, and mitigate the effects of such intrusions when defensive safeguards fail. Indeed, many states have already quietly tightened the slack left

by the federal government and the international community. Whatever else they may be called, most cyber-intrusions are, after all, crimes — which the states are especially well-situated to address.

The federal role

Nothing is more integral to the states' police power than crime prevention. Ensuring the safety of their residents is the core of the states' constitutional responsibilities. Statutes that prohibit and punish fraud, theft, conversion, criminal trespass, forgery, malicious destruction of property, and numerous related offenses all have long been on the states' books. Cyber-intrusions cause and are intended to cause effects that fall within many of those traditional statutes.

Nonetheless, it has somehow come to be assumed that cybersecurity is a federal responsibility. The White House proposed broad new protections in May 2011, but envisioned no role of any significance for state governments. Numerous legislative proposals have been introduced in Congress, but, again, an exclusive federal role is simply assumed. Private studies make the same assumption.

The reasons are understandable. An interconnected and borderless internet means that most activity in cyberspace takes place without regard to state (or international) boundaries. The task of complying with multifarious state cybersecurity laws, each of which could impose varying levels of legal obligation, might easily become burdensome, complex, and costly. Then, too, dealing with threats from abroad has long been seen to be the province of the federal government. It is true that the consequences of a cyberattack that originate overseas can mirror the consequences of a military attack that employs traditional kinetic weaponry; a cyberattack can thus look more like war than crime. That's significant on many levels, not the least of which being that the Constitution prohibits states from making war without congressional approval. Add this to the fact that federal authority has now come to reach so pervasively into the daily lives of all Americans, and it is easy to understand why few notice or even question whether what's being done by the federal government should more properly be done by the states.

And so the federal government has acted — up to a point. Much of applicable federal law predates the notion of cyber-intrusions and simply happens, almost coincidently, to have some relevance. Fraud by wire, radio, or television, for example, has long been a federal criminal offense. Courts have adapted these prohibitions and recognized a variety of means of communications, including facsimile, telex, modem, and internet transmissions, as constituting "wire, radio, or television communication[s]." The Wiretap Act imposes criminal penalties on any person (including law enforcement personnel) who make an illegal interception or who disclose illegally inter-

cepted material. A statute protecting unlawful access to stored communications protects the confidentiality, integrity, and availability of communications stored by the providers of electronic communication services. Other statutes prohibit activities that might be, but are not necessarily, carried out online, such as identity theft. On the other hand, several federal statutes are directed specifically at internet crime. One, for example, prohibits "phishing" (where a defendant uses fraudulent e-mails to obtain bank account numbers and passwords). The CAN-SPAM Act of 2003 provides a means of prosecuting individuals who send vast volumes of unsolicited commercial e-mail.

Easily the most important federal statute, however, is the Computer Fraud and Abuse Act. This single law addresses a number of offenses that relate specifically to computers. It makes it a felony to access classified information in a computer. It makes it a misdemeanor to access financial records or credit history stored in a financial institution. It penalizes the theft of property as part of a scheme to defraud with the use of the computer. It prohibits altering, destroying, or damaging data that belongs to another. All in all, at least 40 additional federal statutes provide grounds for prosecuting cybercrime. Significantly, nowhere in federal law is there any clear indication that any of these prohibitions is intended to preempt any state law.

A borderless internet means that most activity in cyberspace takes place without regard to state or national boundaries.

Three aspects of this federal statutory scheme are noteworthy. First, federal law does little to *prevent* cyber-intrusions. It is aimed almost exclusively at punishing conduct that has already occurred. This is partially the result of offensive asymmetries in cyberspace — attackers need be successful only once, while defenses must be foolproof. But it is also a consequence of policy choices of convenience. It is much easier, bureaucratically as well as legally, for law enforcement agencies to be reactive than proactive.

Preventive technology does exist, but it hasn't been implemented effectively. The federal government's Einstein 2 program, developed by the National Security Agency, is capable of alerting federal computer emergency readiness teams in real time to the presence of malicious or potentially harmful activity in federal network traffic, but thus far the use of Einstein 2 has been limited to federal networks. The next generation of the Einstein programs, Einstein 3, is designed to be employed across the civilian departments and agencies of the executive branch. The program reportedly has the ability to "automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense." Concerns over potential violations of individual privacy, however, have prevented the deployment of the Einstein programs on the public internet. Instead of confronting this problem with creative solutions, perhaps

along the lines of the minimization procedures already written into the Foreign Intelligence Surveillance Act, the federal government has thus far left the private sector to fend for itself.

Where the federal government has been interested in providing security to the private sector, its programs have been poorly constructed. Steps taken to protect critical national infrastructure, such as the Defense Industrial Base Cyber Pilot co-launched by the Department of Defense and the Department of Homeland Security in June 2011, have been limited to the sharing of "threat intelligence" and the "know-how to employ it," but not the monitoring or interception of private-sector communications. The reasons for this hesitation are sensible. As with the Einstein programs, the specter of government surveillance of the internet raises legitimate civil liberties concerns. Federal officials are wary of potential criticism that they have violated the Fourth Amendment prohibition against unlawful searches and seizures. Yet the results of such half-measures are familiar: States, cities, private businesses, and individuals are left to fight their own battles.

Far from taking place in real time, federal response mechanisms continue to be triggered by voluntary notification from victims.

A second key aspect of the current federal statutory scheme is that the federal government makes no meaningful effort to engage in mitigation — at least, again, with respect to nonfederal entities. States and local authorities along with businesses and private individuals must fend for themselves when it comes to alleviating the effects of cyberattacks and cyber-intrusions. Nothing in the current federal statutory framework, for example, brings the resources of the federal government to bear when a financial institution such as MasterCard or PayPal is subject to a botnet attack, as they were when they stopped processing transactions to WikiLeaks. The National Cyberspace Security Response Group, a forum of thirteen principal agencies that coordinate intragovernmental and public/private preparedness operations to respond to and recover from "large-scale" cyber attacks of "national significance," is too cumbersome to react quickly to the kinds of cyber-intrusions that the private sector experiences every hour. Efforts to build a stronger cyber "ecosystem" through the automation and convergence of best cybersecurity practices exist in theory but not in practice. Far from taking place in real time, federal response mechanisms continue to be triggered by voluntary notification from victims; the haphazard nature of federal legislation means that many entities fall through the cracks. The Federal Information Security Management Act, for instance, requires all federal entities to report incidents of data breach, but, for the private sector, different laws apply to different businesses. Health care providers, credit bureaus, and financial institutions all are subject to separate regulatory frameworks — while other industries are left unregulated altogether.

This presages the third element in the federal framework, which is the lack of a comprehensive data protection regime. By adopting the "sectoral approach," federal initiatives impose varying levels of obligation across different industries and omit any mandated cybersecurity requirements for many private-sector entities. But Washington's hopes that private-sector innovation and market incentives will emerge to fill the security gap have failed. The number of intrusions has continued to rise. The offensive asymmetry in cyberspace persists. Ideas for more aggressive protective action abound, but as its sense of insecurity mounts, Washington continues to suppose that any solution must come either from itself or through passive collaboration with private corporations, not the several states. The upshot is lots of talk about the problem, but few, if any, concrete solutions.

State laws

As a result of this juridical void, the states have been increasingly active in taking on cyber-threats. Indeed, recent multistate surveys reveal a surprising volume of computer-related legislation. Every state has enacted laws directed at protecting state governments and businesses specifically from cyber-intrusions. Much of the legislation is remarkably detailed and comprehensive. The beginnings of such legislation can be traced to the California data privacy and breach notification law of 2003. The California law requires state agencies and those conducting business in California — including foreign corporations — to notify a resident of California when personal information concerning that resident has been acquired by an unauthorized person. As of October 2010, 45 additional states had enacted data privacy and breach notification laws.

On the issue of data security and protection (i.e., a "duty to protect" personal information), California has also led the way. In 2004 it enacted a law requiring companies to "implement and maintain reasonable security procedures and practices" to protect personal information about California residents from unauthorized access, destruction, use, modification, or disclosure. At least eight other states have now adopted similar legislation. The statutes, like the earlier, more basic data privacy and data breach notification laws, also apply to entities headquartered outside the state in question — including in foreign countries.

One of the most far-reaching such statutes is Massachusetts's data security act, enacted in 2009. This is one of a number of laws enacted by Massachusetts to curb cyber-intrusions. Because its matrix is likely to be emulated by other states, the law is worth a close look, particularly with regard to its most controversial aspect — extraterritorial application of mandated security programs.

The actual law itself is brief. It merely directs the relevant state agency to adopt regulations to safeguard the personal information of residents of

Massachusetts from unauthorized access. The law then requires that those regulations apply to "any person that owns or licenses personal information about a resident of the Commonwealth." The regulations that have now been promulgated mandate the adoption of a "written information security program" by "any person that owns or licenses personal information about a resident of the Commonwealth." The regulations then prescribe in guidelines what elements the security program should contain. "Personal information" is defined in the regulations to include the resident's Social Security number, driver's license or state-issued identification number, or financial account or credit/debit card number. The text of the statute and the regulations thus make clear that the protections apply to every Massachusetts resident regardless of where that resident is located. This includes those traveling abroad who are even momentarily in contact with a covered person if that person obtains personal information about its resident. (While it extends to those who "receive, maintain, process, or otherwise have access to" personal information, the law does not apply to natural persons who are not engaged in commerce, or to businesses that merely "swipe" but don't retain credit card information so long as the data is handled in accordance with industry standards.)

The plain language of the Massachusetts law therefore clearly gives it extraterritorial application — not only to persons in other states of the Union but other countries as well. Concern about this was expressed by businesses during the administrative hearings prior to the adoption of the regulations. But the law's broad reach survived. Its requirements thus apply, for example, to a restaurant or hotel in Paris that maintains credit card information concerning a Massachusetts resident, since the regulations apply to any persons who "own or license" personal information about Massachusetts residents in connection with the provision of goods or services or in connection with employment. The requirements apply to Air France, the airline on which the resident may have traveled and whose ticket was purchased with a credit card, if that number is stored. And they apply to a small used-book store in Paris that maintains the resident's credit card number for making mail-order or internet purchases. They would apply, indeed, to that book store even if the Massachusetts resident purchased a book through the internet, without ever leaving home in Massachusetts.

With so long an arm, the obvious question arises: Can Massachusetts legally do such a thing?

Legal questions

A NUMBER OF DIFFERENT legal regimes address this question — international law, federal constitutional law, federal statutory law, and Massachusetts's own constitution. The answer is not

simple, but the elements of the analysis go to the essence of what federalism means in the contemporary United States.

Let's begin with international law, if only because the United States Supreme Court famously said in 1900 that "international law is part of our law." What precisely the Court meant by that phrase has been a topic of persistent controversy. One thing that is clear is that treaties, under the Supremacy Clause, are law of the land — provided they are "self-executing," i.e., intended to take effect domestically without implementing legislation. Otherwise, implementing legislation is needed. Thus far only one treaty is in force to which the United States is a party that relates specifically to cyber-intrusions — the Convention on Cybercrime, noted earlier. The Cybercrime Convention requires parties, among other things, to establish laws against cybercrime, to ensure that their law enforcement officials have the necessary procedural authorities to investigate and prosecute cybercrime offenses effectively, and to cooperate with other parties in the fight against computer-related crime. It was negotiated in 2001 under the auspices of the Council of Europe. President Bush signed the treaty and the Senate approved it on August 3, 2006. In his letter of transmittal, the president advised the Senate that the treaty would require no implementing legislation provided the Senate adopted the conditions that he recommended. (It did.) Already, the secretary of state had written in his letter of transmittal to the president, "federal substantive criminal law provides for broad overall coverage of the illegal conduct addressed by the Convention." Importantly, for purposes of the breadth of state authority, nothing in the Convention provides for, let alone requires, the preemption of legislation by sub-national units.

Thus far only one treaty is in force to which the United States is a party that relates specifically to cyber-intrusions.

Any limits on state power to engage in cybersecurity that derive from international law, therefore, must come not from treaty law but from customary international law. It is customary international law that imposes limits on assertions of extraterritorial jurisdiction by both nations and subnational governmental entities within them. It does so though the concept of jurisdiction. Five different "bases" of jurisdiction exist under which rules may be prescribed; two are relevant to the Massachusetts data security law. These are the "territorial principle" and the "passive personality principle." Under the territorial principle, nations can prescribe rules that apply to every person present within their own territory and to conduct that occurs within their territory. Conduct that occurs outside their territory that has effects within their territory can be regulated if those effects are "substantial." Under the passive personality principle, a nation can prescribe rules applicable to conduct that takes place abroad that harms its nationals wherever they might be. The scope of this jurisdictional basis remains uncertain,

though nations have relied upon it in criminalizing acts of terrorism directed against their citizens located abroad.

Citing both principles, nations in recent years have come to assert broad authority to exercise extraterritorial jurisdiction, though not without objection that their rules' reach is "exorbitant." Increasingly, these rules have involved activities on the internet. In one well-known case, a French court held in 2000 that French laws prohibiting Nazi propaganda applied to the operations of Yahoo! — even though its servers were not located in France, none of its personnel were present in France, and the conduct in question did not occur in France. It's anything but clear that the effects of Yahoo!'s operations in France were substantial under the territorial principle, though under an expansive construction of the passive personality principle, a case could be made that some French residents suffered some measure of harm.

Why would it matter whether, say, the state of Massachusetts statute violates customary international law?

But, one might ask, so what? Why would it matter whether the Massachusetts statute violates customary international law? It's unlikely, after all, that any international tribunal would penalize Massachusetts for exercising arguably exorbitant jurisdiction in mandating measures aimed to enhance the data security of its residents. What difference should it make to lawmakers in other states who are considering emulating Massachusetts's approach?

First, as a practical matter, retaliatory legislation is possible. Other nations might put in place similar data security laws protecting their own residents' data from sloppy Massachusetts businesses — or from businesses in other states of the union that have much looser laws. Those states might not be thrilled to bear the brunt of retaliation triggered by Massachusetts. The specter of "principled" retaliation is a relentless diplomatic taskmaster; foreign countries, too, can be made to feel the pain. France's anti-Holocaust laws might have been strengthened in the short term by its court's rigorous enforcement actions, but in the long term the precedent may come back to haunt France as other nations rely upon the Yahoo! case in justifying their own extraterritorial cyber-protection laws.

Second, as a legal matter, violation of customary international law by a state could create domestic legal problems for that state. Recall, again, the U.S. Supreme Court's observation that "international law is part of our law." One theory that is widely (though not unanimously) held among legal scholars is that customary international law is part of federal common law and as such is binding domestically, absent federal legislation to the contrary. If that view is correct, under notions of federal supremacy it would be no great stretch to hold the states responsible for respecting principles of customary international law unless they were permitted by Congress to violate those principles. (It is widely agreed that, for purposes of domestic law,

Congress has the authority to place the nation in violation of customary international law.) There appears to be no case law one way or the other on this question, though in the period following independence from Britain and prior to the advent of the Constitution, some "State" (they were not then states of the union but rather, at least at first, independent nations) courts did apply principles of customary international law as part of their own common law.

As to Massachusetts's own constitution, nothing in it prohibits Massachusetts from violating customary international law. Other state constitutions are similarly silent on the question. While states' common law could conceivably incorporate customary international law, that common law would give way to enactments of the states' legislatures (such as data protection laws), just as federal common law gives way to subsequent federal legislative enactments.

International law is not clear-cut, and no one can say whether the Massachusetts law violates international rules or if it matters.

The short of it is, therefore, that while international law is not clear-cut, no one can say authoritatively that the Massachusetts law violates customary international law or that, if it does, any such violation would have imminent or substantial negative consequences for the state. Unless an international legal prohibition is clear, nations as well as subnational actors are deemed to have freedom to act. Under Massachusetts law, the data security act would thus survive scrutiny even if it violated customary international law's jurisdictional limits.

But what of the United States Constitution? That the law is not clearly prohibited by international law does not mean that it is constitutionally permissible. Nothing in the Constitution prohibits the states from exercising extraterritorial jurisdiction. That jurisdiction might be exercised with respect to activities occurring within another state of the union or within another nation. The Constitution does impose *limits* on the exercise of extraterritorial jurisdiction by states, but those limits are, if anything, more relaxed than the already broad limits set out in international law.

The Constitution's limits are found in the due process clause. Due process requires reasonableness in the exercise of jurisdiction: A defendant is entitled to know whether he should expect to be hauled into court in another state. This traditionally requires minimum contacts with the other state. The phrase "minimum contacts" has been taken to mean that a defendant must "purposefully avail itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws." Requiring minimum contacts protects defendants against litigating in unfair and inconvenient forums and ensures that states do not exceed their jurisdictional limits. But the Supreme Court noted in 1980 that the doctrine has been relaxed substantially in recent years because our contemporary econo-

my is characterized by the conduct of business transactions across both state and national borders without any physical presence. Thus the Court held four years later that the exercise of jurisdiction by California was proper in a defamation suit against a newspaper published outside the state but circulated within it.

Cases concerning jurisdiction over internet activities now arise more frequently, and due process questions loom large. In one of the more insightful judicial opinions on this issue a federal district court suggested a useful way of categorizing web sites. "When a defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the internet," the court said, "personal jurisdiction is proper." However, "when a defendant's internet use involves exchanging information with a host computer, the court must examine the level of interactivity and commercial nature of the exchange in order to determine the propriety of exercising personal jurisdiction." The line between two categories is, unfortunately, not altogether clear. Would Amazon's website, for example, involve the "knowing and repeated transmission" of computer files over the internet, or would it be merely "exchanging information"? Nor is it clear why it should matter that commercial responses to a web advertisement occur by telephone rather than e-mail (or responses embedded within the website). In any event, these are the sorts of considerations that would likely prove relevant in determining whether due process requirements are upheld in the enforcement of the Massachusetts law.

The Supreme Court has struck down state statutes that intrude too far into the sphere of foreign affairs.

Absent the knowing and repeated transmission of computer files, there would appear to be no insurmountable due process problem posed by the Massachusetts law. But what of the possibility of conflict with congressional enactments? If an unavoidable clash arises between state and federal law or if federal law "occupies the field," then the state law is said to be preempted by federal law, which is of course supreme. Here, however, no comprehensive federal legislation on the issue of data privacy and data security currently exists, so no issues of federal preemption arise.

That Congress has not preempted the states from acting in this realm does not, however, mean that the Constitution itself is also silent. In a handful of cases the Supreme Court has held that there exists a "dormant foreign affairs power" that resides exclusively within the federal government — even though Congress has said nothing. Pursuant to this doctrine, the Court has struck down state statutes that intrude into that sphere of foreign affairs which the Constitution entrusts solely to the president and the Congress. A state, the Court opined, may not establish its own foreign policy. The indeterminate scope of the dormant foreign affairs doctrine makes it hard to

apply, but it's enough to note that it has been invoked rarely by the Supreme Court and only with respect to state statutes that represented individual, stand-alone initiatives rather than laws enacted by multiple states directed at vindicating common policy interests.

The constitutional gauntlet does not end here. The Court has also invalidated state laws under the so-called "dormant foreign commerce clause." The Constitution provides that the "Congress shall have Power . . . To regulate commerce with foreign Nations, and among the several States, and with the Indian tribes." The courts have found that this provision not only grants "positive" power to Congress but also imposes "negative" limits upon the states. Obviously the foreign commerce clause does not prohibit every state law that has any effect on foreign commerce. But, as is the case with the dormant foreign affairs power, the states are not permitted to act simply because, on a particular issue of foreign commerce, Congress has remained silent. A state statute such as Massachusetts's must pass two hurdles: It must not discriminate against foreign commerce, and it must not impede the federal government's ability to speak with one voice in foreign affairs. Clearly the first hurdle is overcome, since the statute treats foreign commerce no differently than it treats Massachusetts's own commerce; business concerns within Massachusetts and those located abroad are equally burdened.

Too many state voices mean lots of compliance requirements, which impedes rather than promotes commerce.

The conclusion is less clear with respect to the second hurdle, however. It's at least arguable that Congress, in choosing not to require businesses to adopt written security programs, considers it important that the United States speak with one voice. Multiple state voices mean multiple compliance requirements, which ultimately impede rather than promote commerce by making it too cumbersome for businesses to deal with persons protected by disparate regulatory schemes. Meeting different state program requirements could thus discourage foreign businesses from dealing with Americans, which could become too burdensome. Further, as discussed earlier, the danger of retaliation looms large; one reason for the "one voice" doctrine, the Supreme Court has suggested, is curbing the risk of retaliation against the United States for actions taken by a state. On the other hand, Congress hasn't spoken with *any* voice on the data protection question, let alone one voice, and its silence could be taken as approval of multifarious regulatory schemes. After all, Congress could easily preempt those schemes if it wished to do so.

To whatever extent the dormant foreign commerce clause does pose a problem for the states, it could be possible for states to overcome that hurdle by, as discussed below, moving more squarely into the business of cyber-protection — by becoming what the Supreme Court has regarded as "market

participants." The market participant doctrine, so-called, has its roots in the actual words of the commerce clause. The clause empowers Congress, again, "to regulate Commerce with foreign Nations, and among the several States." Under the doctrine, a state is not subject to the constraints of the commerce clause when it acts as a supplier or producer of goods or services rather than as a regulator. Thus far the Supreme Court has applied the doctrine only to domestic commerce, not to foreign commerce. But it has strongly suggested that the market participant exception does apply to foreign commerce. That would make sense. In a globalized economy, interstate and foreign commerce are all but inseparable, and the market participant exception would be set to naught if the two were evaluated under substantially different constitutional criteria. Lower federal courts seem to have accepted this view.

All in all, then, while the matter is not free from doubt, it cannot be said that any clear legal prohibition or restriction from any relevant body of law clearly prevents a state from enacting a statute such as Massachusetts's data security law.

States and botnets

The apparently unobstructed path through this legal labyrinth has thus made it possible for a growing number of states to mitigate the effects of cyber-intrusions by requiring businesses to adopt data security programs and to notify customers when their personal information is accessed. Mitigation of this sort will also have a deterrent effect, as lower rewards for cyber-intruders diminish the intruders' incentives. The states' legislation represents an important first step in filling a gaping hole in federal law.

Is there something more that the states might do? Might it be possible to leverage their unique lawmaking powers to make money as cyber-defenders? The answer may be yes. A variety of possibilities present themselves. Begin with one of the most prevalent forms of cyber-intrusion — botnet attacks.

Botnets are made up of vast numbers of compromised computers that have been "infected" with malicious code. Once they are infected the botnet computers can be remotely controlled through commands from the "botmaster" to operate in concert to disrupt or block internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code. Because of their versatility, botnets have been described as the "Swiss Army knives of the underground economy." The attacks described above against Estonia and MasterCard, Visa, and PayPal all were botnet attacks. WikiLeaks itself has been the target of botnet attacks. Companies survive these attacks in part by successfully sequestering the malicious traffic and transferring or deflecting it into so-called "sinkholes," "honeypots," and "darknets." Such techniques allow researchers to redirect the malicious

traffic that comes from each client and place it in a research box of sorts, where it can be analyzed and decoded. Unfortunately, most of this takes place after the fact; the sequestration capacity, in other words, is added, *ad hoc*, on the fly, in response to the attacks rather than before them, in anticipation of potential vulnerability. Affected companies must also collaborate with internet service providers (ISPs) in order to sequester the traffic. In some cases the ISPs may be cooperative, while in other situations they may not be.

Here, then, is one place where the states might play a more forceful and potentially profitable role, by instituting, for example, a fee-for-service arrangement that could provide a number of benefits for voluntary subscribers. Subscribers could include almost anyone, including in-state and out-of-state businesses, other states, and potentially foreign businesses and even foreign governments. "Vaccine" programs could be made available to subscribers (and computer "hygiene" made a condition of membership). An early warning system could be put in place to detect incipient botnet attacks on subscribers. Subscribers' servers and computers could be disinfected of zombie malware. Unwitting owners of infected computers joining in the attack could be identified and notified. ISPs could be mandatorily directed by the state to block or shut down compromised computers involved in a botnet. State forensic experts could work with private security firms to attempt to determine the object of the intrusion as well as the identity of the botmasters. States might consider protecting subscribers with active defenses or "electronic fences" for cyberspace, possibly utilizing intrusion detection programs such as Einstein 3, the new shield being put in place by the federal government to protect its own computers. Cooperative arrangements to protect subscribers could be entered into with other stakeholders. Knowing participants in a botnet, when identified, could be prosecuted and, if necessary, extradited. And by engaging in these entrepreneurial efforts the states could qualify constitutionally as market participants, potentially exempting themselves from otherwise applicable limitations flowing from the dormant foreign commerce clause, discussed above.

Continuing to lead the way

Botnets pose one form of cyber-threat; others would require different protective measures. Some will be amenable to state-sponsored remedies while others will not. The point is that a space exists for imaginative, entrepreneurial thinking about potentially profitable cyberdefense by the states. States need not resign themselves to being 18th-century relics in an age of globalized commerce. Opportunities are available for creative rejuvenation. Using traditional police and regulatory powers, states can leverage their unique regulatory and law enforcement assets to succeed where the federal government and the international com-

munity have failed. The result could be a "race to the top" as states compete with one another to provide top-notch cybersecurity for those willing to pay. This strategy has already played itself out within NATO. By capitalizing on its expertise in these matters, the tiny nation of Estonia has been able to mobilize international funding to create the Cooperative Cyber Defence Centre of Excellence, a NATO accredited organization, in Talinn in 2008. The Centre now provides NATO with a wide range of products and services related to cybersecurity, while also serving as an intellectual hub for confronting such threats worldwide.

Cyber-intrusions have caused and will continue to cause widespread harm. Their danger ought not be underestimated. But with innovative thinking on the part of state policymakers, the effect of those intrusions can be mitigated. States already have led the way with data security laws. There is no reason for them to stop here. With the right combination of far-sighted policies and technological prowess, the states might prove, even in a globalized 21st century, to be the effective dual sovereigns that the framers considered essential to preserving and enhancing the security and well-being of the American people.