46 Colum. Hum. Rts. L. Rev. 227

Columbia Human Rights Law Review
Spring, 2015

Article
Scott A. Gilmore[a1]

SUING THE SURVEILLANCE STATES: THE (CYBER) TORT EXCEPTION TO THE FOREIGN SOVEREIGN IMMUNITIES ACT

ABSTRACT

From the hacking of newsrooms to the wiretapping of dissidents, foreign states are infiltrating American computers and intercepting communications--in stark violation of federal law and international norms. So far, the policy debate on cybersecurity has taken it for granted that foreign states enjoy immunity for cyber attacks on U.S. targets. This Article is the first to challenge that assumption.

It argues that the tort exception to the Foreign Sovereign Immunities Act waives the immunity of foreign states for cyber trespass and wiretapping of American computer networks. Showing courts and litigants a roadmap to this new line of litigation, the Article explores the intersection of twentieth century doctrines of immunity with twenty-first century torts. It maps the FSIA's territorial limits onto the geography of cyberspace, and then considers how modern sensibilities conceptualize hacking and eavesdropping as forms of personal injury. Next, it examines whether statutory violations are "torts" for FSIA purposes. Finally, it argues that computer misuse laws and international norms on territorial sovereignty check the discretion of foreign states to surveil U.S. residents.

It closes with a claim for the essential justiciability of cyber tort suits against foreign sovereigns. Using tort law to check governmental excess is central to the Anglo-American legal heritage. In our globally networked era, where Americans are increasingly living under the electronic surveillance of foreign powers, cyber tort ****228*** *suits can serve as a tool to express public values--and limit raw sovereign power--in the contested digital domain.*

INTRODUCTION: THE HACKERS AND THE HACKED

In 2012, Google users around the world received an ominous message: "Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer."[1] These warnings were just the beginning. Two years later, Google security engineers announced that suspected government hackers had infiltrated twenty-one of the world's twenty-five leading news organizations.[2]

Many of these cyberattacks were aimed at the United States. In 2013, the New York Times reported that hackers traced to the Chinese military had repeatedly infiltrated the New York Times' computer systems.[3] Using malware-- malicious software code--the hackers stole the corporate passwords for *every* Times employee and breached a secret Times investigation of corruption in China.[4] The New York Times was not alone; since 2008, the Washington Post, the Wall Street Journal, Bloomberg News, and the Associated Press have been targeted by attacks "intended to uncover the identities of sources for news stories and to stifle critical reports about the Chinese government."[5]

***229** There is nothing new about governments' efforts to "stifle critical reports" by surveilling journalists and seizing their files. Unlawful search and seizure is an ancient tool of censorship. The general writs of King George III sent bailiffs knocking on the doors of eighteenth century English publishers, rooting out libelous papers and their anonymous authors.[6] But surveilling critics was traditionally a domestic matter--a struggle between a polity's government and its critical Fourth Estate.

No longer. State-sponsored hackers are now reaching across borders, and they are not just targeting journalists. Foreign government hackers are engaging in industrial espionage in the United States on a massive scale, stealing terabytes of sensitive data and intellectual property worth billions.[7] In November 2014, Sony Pictures Entertainment experienced a massive cyberattack that destroyed systems and stole large quantities of personal and commercial data.[8] Although a group of hackers calling itself the "Guardians of Peace" claimed responsibility for the attack, the FBI announced on December 19 that the North Korean government was, in fact, responsible.[9] The cyberattack--and a series of threats against Sony employees as well as cinemas showing Sony films--was apparently in response to the scheduled release of *The Interview,* a satirical film lampooning North Korean autocrat Kim Jong-un.[10]

The Sony hack illustrates the problem of "attribution," that is, the difficulty of tracing a cyberattack to its originator.[11] Cyberspace ***230** affords an inherent degree of anonymity--and a range of masking techniques--that allow hackers to obscure their link to a hack.[12] Since a cyberattack can be executed by a loosely affiliated network of actors across geographical borders, there are formidable forensic and jurisdictional barriers to evidence collection.[13] It is perhaps unsurprising, then, that some cybersecurity experts dispute the FBI's conclusion that North Korea perpetrated the Sony hack. Cybersecurity firm Norse Corporation concluded that the hack was more likely an "inside job" carried out by a former Sony employee in collaboration with outside hackers.[14]

If North Korea was indeed involved, the Sony hack is part of a disturbing trend towards states using information technology to censor and surveil civil society and private actors beyond their borders. President Obama voiced shock at a foreign power attempting to silence an American film studio on U.S. soil:

> We cannot have a society in which some dictators someplace can start imposing censorship here in the United States because if somebody is able to intimidate us out of releasing a satirical movie, imagine what they start doing once they see a documentary that they don't like or news reports that they don't like.[15]

Yet those "dictators" are already threatening civil liberties here in the United States, tracking dissidents, monitoring diaspora communities, and compromising human rights investigators. The Ethiopian government has allegedly wiretapped journalists in ***231** Washington D.C.'s Ethiopian community.[16] The Syrian government has reportedly used "spear-phishing" attacks--tricking users to click a fake link to a video of wartime atrocities--to infiltrate opponents of the Assad regime and their international supporters.[17] And hackers apparently aligned with the Vietnamese government have launched malware attacks on staffers at the Electronic Frontier Foundation in San Francisco.[18]

Decades ago, this sort of spying on U.S. targets would have required physically bugging offices and tapping phone lines. But today, spyware, much like unmanned aerial vehicles, permits remote-controlled surveillance. Indeed, a burgeoning "lawful intercept" industry sells digital surveillance tools to a growing market of government buyers.[19] Spyware sold exclusively to governments, such as Remote Control Systems and FinFisher, can infect computers and mobile phones and covertly record e-mails, text messages, phone or Voice over Internet Protocol ("VoIP") calls, and GPS data.[20] They can log keystrokes.[21] They can even activate cameras and microphones to record their environment--converting consumer ***232** devices into remote-controlled surveillance drones.[22] Of course, such spyware can be used for legitimate law enforcement and national security purposes. But it can also silence dissent or steal business secrets.

The targeting of American computer networks raises a novel question: do victims of state-sponsored hacking have any legal recourse against the foreign states behind the attacks? Conventional wisdom says no. Commentators have assumed that foreign governments and their hackers are beyond the reach of American law. Some, like American Enterprise Institute fellow Dan Blumenthal, take it for granted that sovereign immunity shields foreign states from civil suits for cyberattacks.[23] As Marc Rotenberg of the Electronic Privacy Information Center notes, victims "need something more than the federal Wiretap Act to establish jurisdiction."[24]

This Article argues that victims already have "something more"--the tort exception to the Foreign Sovereign Immunities Act ("FSIA") permits cyber tort suits against foreign states that hack U.S. targets.[25] To date, no electronic privacy suit has been brought successfully against a foreign sovereign.[26] And no scholarly work has identified this unexplored chink in the armor of sovereign immunity. This Article lays out a roadmap for how electronic privacy plaintiffs should frame their claims and how courts should decide them.

First, Part I argues that plaintiffs have an arsenal of statutory and common law claims. Computer hacking and electronic eavesdropping within the United States violate the core computer misuse statutes: the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. Each provides a private right of ***233** action and imposes civil liability on governmental entities, both foreign and domestic. These cyberattacks also give rise to common law tort claims for trespass or invasion of privacy.

Part II tackles immunity. It maps how the tort exception to the FSIA, 28 U.S.C. § 1605(a)(5), applies to hacking and electronic surveillance. After laying out the FSIA's framework for determining immunity, it identifies and resolves four novel issues that arise when this twentieth century statute collides with twenty-first century torts. This Part demonstrates four key points: (1) that cyber intrusions into U.S. computer networks meet the territoriality requirement, even if they originate abroad; (2) that the tort exception reaches both common law torts and statutory violations; (3) that invasions of privacy--such as eavesdropping--are personal injuries for FSIA purposes; and (4) that state-sponsored hacking is not a discretionary function entitled to immunity, since it violates clear criminal law and international principles of territorial sovereignty.

Finally, Part III argues for the essential justiciability of electronic privacy claims. Such claims do not challenge a foreign state's surveillance practices within its own territory, and since they invoke statutory rights and rules of immunity, they raise no political questions. On the contrary, common law courts have, for centuries, remedied governmental trespass through the medium of tort law. Today, such suits comport with international limits on sovereign immunity. They expose foreign states to the same risk of litigation in the United States that our government faces for torts it commits in foreign territory and foreign computer networks.

Ultimately, tort suits against foreign states and their hackers are a more effective and less incendiary response to cyberattacks than the alternatives of vigilantism, prosecution, or armed reprisal. Foreign states that break into U.S. computer networks cannot hide behind a veil of immunity: they can and should be held liable. We need only apply the old laws of immunity and tort to the new frontier of cyberspace.

I. CYBER TORTS

The FSIA tort exception requires a tort. Section 1605(a)(5) strips immunity for "tortious acts or omissions" causing "personal injury or death, or damage to or loss of property."[27] This Part argues that electronic privacy plaintiffs can invoke a number of statutory ***234** and common law actions, arising from different aspects of state-sponsored cyberattacks or surveillance. It first surveys the causes of action and then considers whether they are actionable against foreign governmental entities--assuming, for the moment, that immunity can be overcome.

A. From Wiretapping to Electronic Trespass

When foreign state actors intercept communications or infiltrate computers in United States territory, they violate the core computer misuse statutes: the Electronic Communications Privacy Act ("ECPA")[28] and the Computer Fraud and Abuse Act ("CFAA").[29] Coupled with common law torts, these statutes offer a potent arsenal of civil remedies against individuals and governmental entities alike.

Electronic Communications Privacy Act. Comprising three titles, the Electronic Communications Privacy Act of 1986 provides the key protection of communications while in transmission or storage. The ECPA consists of three acts: (1) the Wiretap Act,[30] which prohibits the interception of communications; (2) the Stored Communications Act,[31] which protects stored communications and transaction records; and (3) the Pen Register Act,[32] which regulates analog surveillance techniques such as pen registers and trap and trace devices.[33]

As its name suggests, the ECPA protects communications; but whether a given act of surveillance violates the Wiretap Act or

the ***235** SCA depends on whether the communication was accessed while in transmission or while in storage.

Wiretap Act. The Wiretap Act prohibits the electronic eavesdropping of communications while they are in transit, as well as the use or disclosure of information unlawfully obtained, subject to a few specific exceptions.[34] The Act bars third parties, including governments, from intentionally intercepting or attempting to intercept oral, wire, or electronic communications through the use of any electronic, mechanical, or other device.[35] To be actionable, the interception must have been "contemporaneous with transmission"[36] and the transmission must have occurred through a system that "affects interstate or foreign commerce."[37] Accordingly, courts have found that using malware to reroute e-mail or record communications through Voice-over-Internet Protocol ("VoIP") programs, such as Skype, violates the Wiretap Act.[38] In addition to criminal penalties, ***236** the Wiretap Act creates a civil cause of action against "the person or entity, other than the United States," that violates the Act.[39]

Stored Communications Act. While the Wiretap Act protects communications in transit, the Stored Communications Act ("SCA") protects communications held in storage by an Internet Service Provider ("ISP").[40] The SCA makes it a federal offense to intentionally access, without authorization or in excess of authorization, a "facility through which an electronic communication service is provided," and obtain or alter a communication while it is held in storage.[41] Like the Wiretap Act, the SCA authorizes civil actions.[42]

The SCA has a fairly narrow application for victims of state-sponsored cyberattacks. Since the Act is limited to providers of "electronic communication services" or of "remote computing services," the SCA generally only protects data on servers, not on personal computers.[43] This means that the SCA would come into play if, for example, a hacker obtained unauthorized access to e-mails stored on the server of a webmail provider like Google or Yahoo.[44] But it would not apply if the same e-mail were intercepted in transit after the user hits "send," nor if it were accessed while saved on the user's ***237** computer. However, such an intrusion into a personal computer could be actionable under the Computer Fraud and Abuse Act.

Computer Fraud and Abuse Act. The CFAA is essentially a computer trespass statute. Section 1030(a) of Title 18 imposes criminal penalties on anyone who "accesses a computer without authorization or exceeds authorized access and thereby obtains ... information from any protected computer."[45] The CFAA also provides a private right of action if a violation of the Act causes loss or damage: to state a claim under § 1030(g), a plaintiff must allege (1) damage or loss[46] (2) caused by (3) a violation of one of the substantive provisions in 18 U.S.C. § 1030(a)-(b) and (4) conduct involving one of the factors in § 1030(c)(4)(A)(i)(I)-(V).[47]

The CFAA has been frequently maligned by civil liberties advocates, and deployed by prosecutors, due to its breadth. The term "protected computer" includes any computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[48] Similarly, courts are divided on just how broadly they should read the terms "access without authorization" and ***238** "exceeds authorized access."[49] Much of the debate turns on whether exceeding authorized access is limited to breaching code-based access restrictions *(e.g.,* password protections), or whether it also includes breaching contract-based use restrictions *(e.g.,* terms of service agreements).[50]

For present purposes, the less controversial concept of "access without authorization" covers most state-sponsored cyberattacks. Infiltrating computers through malware is squarely within the concept of "hacking" that Congress had in mind. Indeed, the Senate Judiciary Committee report accompanying the 1996 amendments to the CFAA cited cases of foreign-based hackers infiltrating U.S. computers.[51] More recently, courts have applied the CFAA to hacking techniques including "phishing" schemes,[52] "Trojan Horse" infections,[53] "spoofing" IP addresses,[54] and taking remote control of root passwords.[55]

239** ***Common law trespass and invasion of privacy. Beyond the core federal computer crime statutes, electronic privacy plaintiffs can also invoke common law torts under state law. Following the 1890 work of Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*,[56] nearly all fifty states have recognized a cause of action for privacy violations.[57] Foreign digital surveillance or cyberattacks can give rise to a tort action against anyone "who intentionally intrudes, physically or otherwise, upon the solitude" or "private affairs" of another, so long as "the intrusion [would] be highly offensive to a reasonable person."[58] Indeed, courts have found that electronic snooping, such as installing a keylogger, is a cognizable

intrusion.[59]

Similarly, a number of states permit trespass to chattels actions where the only contact with the plaintiff's property is through electronic signals.[60] In the seminal case, *Intel Corp. v. Hamidi,* the Supreme Court of California translated this ancient tort into the cyber context, holding that a trespass through electronic signals is actionable if it "damages the recipient computer" or "impair[s] its functioning."[61] In the electronic context, this damage or impairment need not occur through traditional physical means; the tort does not require physically smashing a hard drive or cutting cords. Malicious ***240** code or even a barrage of spam e-mail can interfere with the functioning of a computer system. Thus, in *CompuServe Inc. v. Cyber Promotions, Inc.,* the Southern District of Ohio, applying *Hamidi,* held that the element of actual harm could be established by the fact that "multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment," and hence diminish its value to the owner. The upshot is that a trespass to chattel can consist only of electrons, although some states have yet to recognize a cause of action for cyber-trespass.[62]

Finally, there are a variety of state wiretapping and anti-spyware statutes that could be brought to bear against state-sponsored cyberattacks.[63] For example, California's Anti-Phishing Act of 2005 authorizes civil actions against persons who obtain private information by falsely posing online as a business.[64] But not all state privacy laws authorize private enforcement.[65] Moreover, plaintiffs may face a distinct hurdle with state law claims; given the potential impact on foreign affairs, litigating trans-border cyberattacks under state privacy laws may invite preemption challenges.[66]

Of course, the focus so far has been on trespassory or privacy torts; but the harms caused by cyberattacks can extend beyond breached privacy and a sluggish hard-drive--disabling a computer system that runs essential infrastructure could threaten life and limb. To date, no known cyberattack in the United States has caused physical injury, but one should not rule out the possibility that ***241** interfering with a power grid or water treatment facility could result in physical harm or death, with all the ensuing legal consequences.

TABLE 1: OVERVIEW OF STATUTORY AND COMMON LAW CLAIMS

CIVIL ACTION	PROHIBITED CONDUCT	APPLICATIONS
Federal Wiretap Act, 18 U.S.C. § 2520 *et seq.*	Electronic eavesdropping of communications in transit	E-mail re-routed by spyware; Re-routing or recording of Voice over Internet Protocol (*e.g.,* Skype)
Stored Communications Act, 18 U.S.C. § 2701 *et seq.*	Unauthorized access to electronic communications held in storage with an ISP	Accessing e-mail archived on webmail server (*e.g.,* Gmail, Facebook); Accessing data in the "cloud" (*e.g.,* Google Drive)
Computer Fraud and Abuse Act, 18 U.S.C. § 1030	Obtaining information or causing damage via unauthorized access to a protected computer	Trojan Horses; Phishing schemes; Key-loggers; IP spoofing; Hacking root passwords
Intrusion Upon Seclusion	Intentional invasion of privacy if highly offensive to a reasonable person	Key-loggers; Remote control of webcam or microphone
Trespass to Chattels	Intentional interference with a computer that impairs its functioning or diminishes its value	Website scraping; Spyware installation

***242 B. Governmental Entity Liability: Dispensing with a Red Herring**

We have seen that electronic privacy plaintiffs have a range of remedial tools, from federal statutory actions to common law

tort claims. But do these laws impose liability on governmental entities? Note that this question is analytically distinct from whether a defendant is immune from jurisdiction. A state might have waived its sovereign immunity, yet face no liability under a statute that is limited to individuals. So foreign sovereigns will likely argue that they are simply not part of the class of potential defendants.

Courts should not be distracted by this red herring. There are two paths that resolve the issue, and both reach the same conclusion: foreign governmental entities are amenable to suit, so long as immunity can be overcome.

First, the FSIA may itself offer a general answer. Section 1606 provides that "[a]s to any claim for relief with respect to which a foreign state is not entitled to immunity ..., the foreign state shall be liable *in the same manner and to the same extent as a private individual* under like circumstances."[67] One plausible reading of this provision is that once a foreign state is stripped of immunity, it becomes by operation of law, a private individual for purposes of liability.

The Supreme Court seems to have embraced this view: "Where state law provides a rule of liability governing private individuals, the FSIA requires the application of that rule to foreign states in like circumstances."[68] And lower courts have followed suit, holding that "Section 1606 acts as a 'pass-through' to substantive causes of action against private individuals that may exist in federal, state or international law."[69] This "pass-through" has permitted ***243** claims against foreign states that range from state common-law and statutory causes-of-action, such as wrongful death,[70] to federal statutory causes-of-action, including civil claims under the Racketeer Influenced and Corrupt Organizations Act ("RICO")[71]

The FSIA's limited legislative history also suggests that Section 1606 is best read to treat foreign-state defendants as if they were private individuals. The reports of the House and Senate Judiciary Committees emphasize that 1606 was intended to subject foreign states to the same rules of tort liability as private parties, except with respect to punitive damages:

> Section 1606 makes clear that if the foreign state, political subdivision, agency or instrumentality is not entitled to immunity from jurisdiction, liability exists as it would for a private party under like circumstances. However, the tort liability of a foreign state itself, and of its political subdivision (but not of an agency or instrumentality of a foreign state) does not extend to punitive damages.[72]

Nonetheless, there is a limit to the power of Section 1606 to expand the scope of liability for underlying causes-of-action. Some statutes define a limited class of defendants. The Torture Victim Protection Act (TVPA), for example, authorizes a cause-of-action against "[a]n individual" who subjects victims to torture or ***244** extrajudicial killing.[73] Because the TVPA refers only to "individuals," several judges on the U.S. District Court for the District of Columbia have refused to apply the TVPA to foreign states through Section 1606.[74] In *Holland v. Islamic Republic of Iran,* the court cautioned against overriding Congress' intent to limit the TVPA to foreign officials and officers.[75] In *Holland* and another decision, *Dammarell v. Islamic Republic of Iran,* the court heeded the Senate Report's admonition that the TVPA "uses the term 'individual' to make crystal clear that foreign states or their entities cannot be sued under this bill under any circumstances: only individuals may be sued."[76] These cases suggest a rule that statutes of general (or ambiguous) application, such as RICO, can apply to foreign states through Section 1606, while statutes that confine their scope to individuals cannot be expanded to reach states or other entities.

Holland and *Dammarell's* treatment of the TVPA suggests that courts applying Section 1606 should look to the underlying cause of action to determine if it applies to governmental entities, or if, like the TVPA, it is confined to individual liability. Even under this approach, though, most electronic privacy claims would pass muster since, as we will see, the core computer misuse statutes apply to governmental entities.

1. Entity Liability under the ECPA: Wiretap and Stored Communications Claims

To determine whether ECPA claims can apply to foreign states, we must examine the history of the Wiretap Act and how its scope grew intertwined with that of the Stored Communications Act through a series of amendments.

***245** When first enacted in 1968, the federal Wiretap Act--originally Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Crime Control Act")[77]--was confined to a limited class of defendants. Under the Crime Control Act, Section 2511 of title 18 imposed criminal penalties on "[a]ny person who ... willfully intercepts ... any wire or oral

communication."[78] In turn, Section 2520 of the Crime Control Act also created a civil liability regime, giving "any person whose wire or oral communications is intercepted ... a civil cause of action against any person who intercepts ... such communications."[79]

Thus, only a "person" was subject to the criminal penalties of Section 2511 or the civil liability of 2520. And Section 2510 defined the term "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."[80] In short, the original Wiretap Act applied only against individuals or private business entities, not state entities.

All this changed with the enactment of the Electronic Communications Privacy Act of 1986.[81] First, the ECPA expanded Section 2511 to cover "any wire, oral, or electronic communication."[82] Second, the ECPA amended the civil liability provision, Section 2520, adding the words "or entity" to those who may be sued.[83] Finally, the ECPA enacted the Stored Communications Act, codified at 18 U.S.C. §§ 2701-2712, creating civil liability for unlawful access to stored electronic communications.[84] Using language identical to Section 2520 of the Wiretap Act, Section 2707(a) of the Stored Communications Act authorized a civil cause of action against "the person or entity" that engaged in the violation.[85] The ECPA, however, did not define the term "entity."[86]

***246** Even so, the Act's text and legislative history strongly suggest that "entity" was intended to include governmental entities. As one court observed, "the addition of the words 'entity' can only mean a governmental entity because prior to the 1986 amendments, the definition of 'person' already included business entities.[87] In other words, "entity" must be read to include governments because it would otherwise be superfluous.

The legislative history expressly says as much. The Senate Committee Report accompanying the ECPA makes it clear that the term "entity" was added to § 2707(a) of the Stored Communications Act to enable plaintiffs to sue *governmental* entities:

> [A]ny provider of electronic communication service, subscriber, or customer of such service aggrieved by any violation of this new chapter may recover from any person or entity--*including governmental entities*--who knowingly or intentionally violated this chapter.[88]

Although the Report does not explain why the ECPA also added "entity" to the Wiretap Act's civil liability section, there is no indication that Congress intended "entity" to mean two different things in these parallel sections. Thus, the Report's comment on the scope of "entity" for the SCA also explains the scope of "entity" for the Wiretap Act.

That "entity" includes governments was made all the more clear when Congress once again amended both Acts in 2001, this time to shield the United States from civil liability.[89] Thus, using identical language, the Wiretap Act and Stored Communications Act both authorize civil actions against "the person or entity, other than the United States, which engaged in [the] violation."[90] There would have been no reason to carve out an exception for the United States if governments could not be sued. So Congress clearly understood that the 1986 amendments to both Acts created governmental entity liability.

Most courts that have examined the issue have agreed.[91] Leading the pack, the Second and Sixth Circuits have recognized ***247** governmental entity liability under both acts for three reasons. First, as the Sixth Circuit explained in *Adams v. City of Battle Creek,* the terms "or entity" in the 1986 amendments must refer to governmental entities in order to have meaning and effect: business entities had already been covered for nearly two decades.[92] Second, as the Second Circuit noted in *Organizacion JD Ltda. v. U.S. Department of Justice,* the legislative history for the SCA's parallel civil-liability section "specifically references 'governmental entities' as potentially liable."[93] This congressional statement should be read to apply to both the SCA and the Wiretap Act, since statutes *in pari materiae* are to be interpreted together, to form a coherent body of law.[94] Finally, the use of different terms in the criminal and civil provisions of the Acts indicates that Congress intended different regimes of liability--a civil one that applies to all individuals and entities other than the United States, and a criminal one that applies only to individuals and businesses.[95]

Only the Seventh Circuit has held otherwise, concluding that governmental entities are excluded from civil liability for intercepts in violation of § 2511(1) of the Wiretap Act, although they have no such immunity for violations of the Stored Communications Act.[96] The Seventh Circuit's analysis in *Seitz v. City of Elgin* has all the false appeal of the deceptively simple. First, the court reasoned, the Act's criminal prohibition of unlawful intercepts only permits the criminal prosecution

of a "person."[97] Second, § 2510(6) excludes ***248** governmental entities from the definition of "person."[98] From this, the court concludes that only a "person"-- meaning an individual or private business--can violate § 2511(1).[99] And if only a "person" can violate section 2511(1), then only a "person" can be sued for such violation.[100] In the Seventh Circuit's view, an intercept committed by a governmental entity simply does not violate the statute.

The problem is that governmental entities, as legal abstractions, do not commit wiretapping. Their human agents do. And when they do so without a warrant, or other dispensation, they violate the Act. The only issue is whether liability for that violation can be attributed to the principal--the government itself. And the statute expressly answers that. For criminal liability, the answer is no. Per § 2511(1), only a "person" can be subjected to fine or punishment under § 2511(4). So a government cannot be prosecuted for its agents' unlawful intercepts.

But for civil liability, the answer is yes. By creating a cause of action against a "person or entity," § 2520 necessarily directs that those legal fictions can be held civilly liable for the wrongful acts of their human agents. In short, *Seitz* misinterprets Congress' decision to exempt governmental entities from criminal liability as a decision to insulate those entities from tort liability.

The majority approach is thus the better one: civil liability for government entities is more faithful to the text and history of the Wiretap Act, and more attuned to its purpose. One of Congress' chief concerns animating the ECPA was to "guard against the arbitrary use of Government power to maintain surveillance over citizens." Taking an eraser to Title I and shielding government entities from suit does not do justice to that goal.

Yet there is still a further bridge to cross. Even if the Wiretap and Stored Communications Acts apply to governmental entities, do they apply to *foreign* states? To date, all cases addressing the scope of liability under § 2520 have been suits against local and municipal governments, not foreign powers. But nothing in the text or history of either Act precludes suits against foreign governments.

The text of the ECPA is devoid of any qualifying language that would imply that foreign states were to be excluded from civil liability. The Wiretap Act and SCA both leave the term "entity" undefined, and only mention "foreign powers or agents of a foreign ***249** power" with reference to the targets of U.S. government surveillance.[101] And the legislative history offers little further guidance. The House report makes only one oblique reference to surveillance by foreign powers, cautioning that although the technology to intercept microwave telephonic communications is expensive and difficult, "the practice is sufficiently well known as to be an option for satellite dish owners and for foreign intelligence agencies."[102] At a minimum, this suggests that Congress was aware that foreign powers were potential violators of the Act. Otherwise, the House and Senate Committee Reports make no reference to surveillance by foreign states.[103]

Given the dearth of textual or legislative evidence, courts are likely to draw on principles of statutory construction. As a first observation, there is no presumption against *extra-nationality;* that is, there is no canon of statutory construction that compels interpreting a generally worded statute to apply only to U.S. entities or nationals.[104] There is, of course, the canon against the extraterritorial application of federal statutes.[105] This canon may in practice bar the application of U.S. law to the acts of some foreign actors, but not to those taken within U.S. territory.[106]

There is thus no basis for courts to add a foreign state exemption that Congress did not see fit to include in the text of the statute. As then-Circuit Judge Blackmun once noted, "if the Congress [had] intended to provide additional exceptions, it would have done so in clear language."[107] This principle is all the more compelling when we consider that Congress did provide one clear exception to ***250** government entity liability: the 2001 amendments to the ECPA shielded the U.S. government from civil liability. Congress knew how to create a safe harbor for certain government defendants when it twice amended the Acts, yet it chose not to shield foreign states. Indeed, the inclusion of one safe harbor implies the exclusion of the other. In the end, defendants will no doubt try to rewrite the ECPA to exclude foreign governments, but the text and history of the law simply do not support that construction.

2. The Computer Fraud and Abuse Act

The case is even stronger for the Computer Fraud and Abuse Act: it explicitly applies against foreign states, though in a circuitous manner. Section 1030(g) provides a civil action "against the violator." And the Act makes clear that "persons" can be "violators," by providing for forfeiture against "any person convicted of a violation."[108] Further, it defines a "person" to

include a "governmental entity,"[109] including "any foreign country, and any state, province, municipality, or other political subdivision of a foreign country."[110] So through this daisy chain of definitions, the CFAA contemplates that foreign sovereigns can violate the Act and be held civilly liable. Indeed, the United States has itself interpreted the CFAA to apply against foreign governmental actors who hack U.S. computers: in May 2014, the Department of Justice sought and received a federal grand jury indictment of five generals of the Chinese People's Liberation Army on multiple counts of CFAA violations.[111]

3. Government Entity Liability at Common Law

Finally, there is no doubt that foreign states can be held liable in tort at common law. FSIA case law is replete with cases applying common law torts to foreign states and their agencies or subdivisions. State common law has provided the cause-of-action in cases under the FSIA in every category of damages action where the defendant is a foreign state, from wrongful death and battery,[112] to *respondeat* ***251** *superior*,[113] negligence,[114] and trespass theories.[115] Cyber-trespass should be no different.

In sum, victims of unlawful surveillance or cyberattacks have a range of substantive rights of action. And these rights can be invoked against governments, both foreign and domestic. The real hurdle will be overcoming foreign sovereign immunity.

II. THE (CYBER) TORT EXCEPTION TO THE FOREIGN SOVEREIGN IMMUNITIES ACT

This Part shows how courts should apply the FSLA tort exception to waive immunity when foreign states hack U.S. computers in clear violation of U.S. law. It first examines how the FSLA framework operates. It then discusses how electronic privacy claims can satisfy four key elements of the tort exception: territoriality, a cognizable tort, a cognizable injury, and a non-discretionary governmental act.

The FSIA starts from a presumption that foreign states are immune from suit and then carves out exceptions to that rule.[116] Applying the Act to a foreign state entails a three-step process: first, section 1604 makes clear that claims against foreign states are potentially subject to immunity.[117] Determining which suits are subject to the FSIA is accomplished largely through the Act's definitions section. For example, a foreign state is defined to include a ***252** "political subdivision" or "an agency or instrumentality,"[118] but not individual officials.[119] Foreign states are thus covered by the immunity regime, while individuals are not.

Second, sections 1605 through 1607 list all claims that are exempt from immunity, including the tort exception.[120] Once immunity is denied, section 1330 provides both personal jurisdiction--assuming proper service[121]--and subject-matter jurisdiction.[122] This three-step process provides "the sole basis for obtaining jurisdiction over a foreign state in our courts."[123]

Our present concern is the tort exception, 28 U.S.C. § 1605(a)(5), which denies immunity to a foreign state in cases:

> [I]n which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment; except this paragraph shall not apply to
>
> (A) any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused, or
>
> (B) any claim arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights.[124]

Thus the essential elements to the tort exception are: (1) a non-commercial tortious act or omission[125] (2) committed by a state or ***253** its agents that (3) causes personal injury or property damage (4) occurring in the United States, and that is not (5) an exercise of a discretionary function or (6) one of the specifically exempted types of claims.[126]

On its face, the exception to immunity is drafted broadly. The House Report notes that although Congress was "directed primarily at the problem of traffic accidents," it "cast" the exception "in general terms as applying to *all* tort actions for money damages."[127] Despite this broad legislative grant, courts often follow the influential D.C. Circuit's practice and construe the exception narrowly "so as not to encompass the farthest reaches of common law."[128] This Part guides courts on how to navigate these mixed signals. While electronic privacy claims may present difficult issues, there is no reason why traditional torts based on novel technologies should not proceed.

A. Territoriality: Locating a Cyber Tort

The tort exception is limited to torts occurring in the United States.[129] As a practical matter, this screens out a number of ***254** electronic privacy cases and ensures that U.S. courts are not a court of claims for global privacy rights.[130] But it does not bar all claims for cross-border cyberattacks on U.S. targets.

When foreign states infiltrate computer networks located in the United States, they commit torts in U.S. territory. True, these cyberattacks might be planned and directed from outside the United States, but the act that proximately causes injury--the intrusion or interception--occurs here. In the case of Doe *v. Ethiopia,* for example, copies of a FinFisher spyware suite linked to Ethiopian government servers had been surreptitiously installed on the personal computer of a U.S. citizen at his home in Silver Spring, Maryland.[131] The device intercepted his family's communications in the United States by remotely activating his computer's microphone, redirecting e-mails, and recording web browser information to his local hard drive.[132]

U.S. computer networking infrastructure is also being used to re-route wiretapped data to foreign governments. In February 2014, the Canadian research group Citizen Lab discovered that at least ten foreign countries were using proxy servers located in the United States to "launder data from infected computers back to the government operator" of a spyware suite called Remote Control System.[133] These complex, transnational chains of digital surveillance involve serious unlawful conduct in the United States.

When it comes to such cross-border torts, courts generally apply the tort exception whenever a substantial part of the acts or omissions occurs in the United States.[134] They may differ on the ***255** formulation of the standard, but not on its application. For the D.C. Circuit, the "essential locus" of the tort must occur in the United States--suggesting that at least some conduct could occur overseas. In *Asociacion de Reclamantes v. United Mexican States,* the court held that the exception did not cover claims that Mexico had failed to compensate American landowners for seized property as required by a claims-settlement treaty.[135] The claims were for breaching the treaty--not for trespass--and the decision to breach was made entirely in Mexico.[136] The "essential locus" of the tort was therefore outside the United States.[137]

Similarly, the Ninth Circuit requires that a cross-border chain of events must involve "at least one entire tort occurring in the United States."[138] In *Olsen v. Government of Mexico,* the court considered the case of a Mexican government plane that had crashed north of the border while transferring prisoners.[139] Plaintiffs brought wrongful death claims, alleging that the crash was caused by negligent piloting in U.S. airspace, and by negligent maintenance and direction back in Mexico.[140] The court was satisfied that the allegation of negligent piloting gave a sufficient basis for jurisdiction.[141]

The analytic point is that both the D.C. and Ninth Circuit approaches would apply the tort exception to a trans-border chain of events, whenever at least one event occurring in the United States could stand alone as a tort.[142] As the Ninth Circuit observed, a stricter rule would invite artful pleading by defendants, since "requiring every aspect of the tortious conduct to occur in the United States ... would encourage foreign states to allege that *some* tortious conduct occurred outside the United States."[143]

***256** For a powerful illustration, consider two cases of assassinations carried out on U.S. soil. *Letelier v. Republic of Chile* and *Liu v. Republic of China* both involved political killings that were planned abroad but executed in the United States by foreign agents.[144] In *Letelier,* the regime of Chilean dictator Augusto Pinochet arranged the assassination of a former Chilean

diplomat and his American aide through a car bombing in Washington D.C.[145] In *Liu,* gunmen in California were alleged to have killed a San Francisco resident under orders from a Taiwanese intelligence official.[146] In both cases, the courts applied the tort exception, even though the tortious acts in the United States were initiated through a chain of events overseas.[147]

Both *Letelier* and *Liu* are consistent with the Supreme Court's recent jurisprudence on the presumption against the extraterritorial application of federal statutes. As the Court explained in *Morrison v. National Australia Bank, Ltd.,* the threshold question is whether the conduct that is the "focus of Congressional concern" occurred within U.S. territory.[148] The fact that some collateral acts occurred on U.S. soil does not necessarily make a claim territorial, nor does collateral foreign conduct always render a claim extraterritorial. There is thus a helpful symmetry between the *Morrison* "focus" test and the approaches taken by courts in the FSIA tort exception context: both look to whether the conduct specially-regulated by a statute (or common law rule of decision) substantially occurred in the United States.[149]

***257** Thanks to this symmetry, the assassination cases provide compelling analogies for cross-border cyber torts. In both instances, foreign states intentionally target victims in the United States. And they do so through coordinated operations that are executed in U.S. territory but directed from abroad. The difference? In the 1980s and 1990s, foreign states had to rely on human agents to infiltrate U.S. borders. Today, they can use remote-controlled malware--or, for that matter, drones--to accomplish the same ends.[150]

Spyware functions much like a remote-controlled drone. One spyware platform popular among foreign states is "Remote Control System" or "RCS."[151] Once installed on a target device, RCS phones home to command-and-control servers.[152] RCS can be remotely instructed to activate a webcam or microphone and transmit a recording back to its command-and-control server.[153] In effect, the ***258** spyware converts a personal computer into a surveillance drone, capable of recording its physical environment. The analogy to drones is instructive: would *Letelier* really have come out any differently if the assassination had been committed by drone strike?

Courts should see cyber intrusions for what they are: the functional equivalent of physical trespass within the United States.[154] The Supreme Court long ago adopted this functional approach in the seminal case *Katz v. United States,* noting that a "surveillance technique" that "involve [s] no physical penetration" can still be an invasion of privacy.[155] And the Court continues to analogize technological surveillance to trespass, analyzing whether thermal imaging of interiors renders possible what once would have required a physical invasion and therefore constitutes a search.[156]

In trespass, the "essential locus" of the tort is the place where the property is found.[157] Thus, by installing code on a hard drive located in the United States, the foreign state has committed a form of trespass in U.S. territory. Accordingly, the first court to address the issue found that the CFAA protects computers in the United States from hackers physically located overseas and that such protection involves no extraterritorial application of the law.[158] In ***259** *United States v. Ivanov,* the United States prosecuted a Russian hacker who infiltrated a Connecticut business's computer network to obtain its "root" passwords.[159] The court held that the violation occurred in U.S. territory because the accessed computers were housed in Connecticut: it didn't matter that they "accessed by means of a complex process initiated and controlled from a remote location."[160]

In sum, a cyberattack initiated from abroad should be analyzed like other cross-border torts that are planned overseas but executed in U.S. territory. As the *Ivanov* court found, the violation occurs where the intrusion takes place. A cross-border cyberattack on a U.S.-based computer occurs in the United States for FSIA purposes.

B. Tortious Acts: The Statutory Torts of Interception and Unauthorized Access

Wiretap Act or CFAA claims will also raise a second question: does the FSIA tort exception apply to statutory violations?

No court has squarely addressed the issue. In fact, tort exception cases involving statutory violations are surprisingly few. The Second and Ninth Circuits have applied the exception to statutory violations without reservation or analysis. In *Doe v. Bin Laden,* the Second Circuit held that claims arising under the Anti-Terrorism Act[161] fell within the tort exception and warranted jurisdictional discovery.[162] The court had "no doubt that the terrorist acts giving rise to the harms at issue--aircraft sabotage, extrajudicial killing, and conspiracy to support the same--are all torts."[163] Similarly, in *Liu v. Republic of China,* the

Ninth Circuit applied the tort exception to claims for wrongful death, without pausing to consider the scope of the words "tortious act."[164]

These courts were right not to pause. The text, history, and purpose of the FSIA suggest that statutory torts are cognizable. First, although the text of § 1605(a)(5) refers to a "tortious act or omission" without defining the term "tortious," the provision explicitly refers to ***260** "personal injury *or death*."[165] Since the tort of wrongful death is "purely a creature of statute," the FSIA must embrace at least one statutory tort.[166] Any contrary reading that limits the exception to common law torts would render this reference to "death" pointless. And reading "death" as surplusage is impermissible, as Chief Justice Burger observed: "In construing a statute we are obliged to give effect, if possible, to every word Congress used."[167] So, if Congress intended 1605(a)(5) to reach wrongful death, then it must have intended the Act to reach statutory torts.

Ordinary usage suggests the same. Because the text of the FSIA does not define "tortious," we must look to the word's ordinary legal meaning.[168] That meaning encompasses both common law and statutory torts; *Black's Law Dictionary* defines a "tort" as a "[1] civil wrong, other than breach of contract, for which a remedy may be obtained, [usually] in the form of damages; [or 2] a breach of a duty that the law imposes on persons in particular relation to one another."[169] Nothing in *Black's* limits a "tort" to the breach of a *common law* duty. On the contrary, *Black's* definition of "tort" includes any redressable violation of the Constitution.[170] So a redressable statutory violation is a type of tort.

This ordinary meaning is consistent with common law principles. As the Supreme Court explained, the hallmark of a tort is its remedy: "[r]emedial principles ... figure prominently in the definition and conceptualization of torts."[171] What makes an act ***261** "tortious" is not the *source* of the legal duty breached, but rather "the availability of ... damages to compensate the plaintiff 'fairly for injuries caused by the violation of his legal rights.'"[172] Since violations of the ECPA or the CFAA are redressable civil wrongs, they must be "tortious" for FSIA purposes.

It would be hard to square any other interpretation with the purpose of the FSIA. The Committee Reports make it clear that Congress "cast" the tort exception "in general terms" and intended it to reach *"all* tort actions for money damages."[173] This broad scope accords with the Act's underlying aim to remove immunity for torts committed in U.S. territory and to ensure uniformity and predictability in foreign sovereign litigation.[174]

Reading statutory torts out of the FSIA tort exception would throw immunity law into disarray. This is because, in many states, tort law is now a creature of statute. If we were to read statutory torts out of the Act, much of California tort law would fall outside of the immunity exception. Section 1708 *et seq.* of the California Civil Code, which codifies torts for battery and other wrongs, would be off-limits.[175] Ditto for the District of Columbia, where a plaintiff seeking damages for death caused by negligence must invoke § 16-2701 of the D.C. Code.[176] Even more absurd would be Louisiana, where *all* tort law is a creature of statute. Article 2315 *et seq.* of the Louisiana Civil Code codifies all tort claims.[177] With that state's civil law legacy, even negligence would not be cognizable under the FSIA tort exception.[178]

To grasp how this absurd result runs counter to congressional intent, consider the traffic accident. We know from the legislative ***262** history that originally "Section 1605(a)(5) [was] directed primarily at the problem of traffic accidents ...,"[179] Yet no foreign sovereign could ever be sued in Louisiana for its agents' negligent driving, since negligence is a statutory tort in that state. This absurd result undermines Congress' effort to achieve nation-wide uniformity in foreign sovereign litigation, since a foreign state's immunity under section 1605(a)(5) would vary state-by-state, depending on whether that state has chosen to codify its torts.[180] In short, a close study of the text, history, and purpose of the FSIA confirm that statutory torts must be cognizable.

C. Privacy Invasion as Personal Injury

The tort exception applies only to actions "for personal injury or death, or damage to or loss of property."[181] The property clause clearly covers claims involving damage to computers, but what about claims such as wiretapping or intrusion upon seclusion, where no physical injury or property damage can be shown? Is a violation of privacy a "personal injury" for purposes of the FSIA?

To date, only one court has addressed a privacy claim under the tort exception. In *Alpha Therapeutic Corporation v. Nippon*

Hoso Kyokai, the Ninth Circuit presumed, without further analysis, that invasions of privacy are cognizable under § 1605(a)(5). There, a plaintiff sued a Japanese public television company for invasion of privacy after he was interviewed by a reporter wearing a concealed wire recorder.[182] The Ninth Circuit held that the plaintiff had made out a well-pleaded privacy claim and that subject matter jurisdiction was proper under the FSIA tort exception.[183] Without explicitly recognizing that an invasion of privacy is a "personal injury" for the FSIA purposes, the court implicitly accepted as much by allowing the claim to proceed, since it evidently did not involve damage to or loss of property.

***263** Further analysis of the statutory text is in order. The FSIA does not define "personal injury," so the term is best construed "in light of the common law."[184] The phrase's ordinary legal meaning includes both physical injury and moral damages, such as mental or reputational harm. *Black's Law Dictionary* defines "personal injury" to include "[a]ny invasion of a personal right, including mental suffering and false imprisonment."[185]

Courts in other contexts have agreed. In *Bernstein v. National Broadcast Company,* the U.S. District Court for the District of Columbia determined that a violation of privacy is a personal injury for purposes of choice of law: "the mind of an individual, his feelings and mental processes, are as much a part of his person as his observable physical members ... [a]n injury ... which affects the sensibilities is equally an injury to the person as an injury to the body."[186] Following *Bernstein,* trial courts in the District of Columbia continue to hold that "[i]nvasion of privacy is a personal injury--an injury to feelings."[187]

They are not alone. The "gravamen of the action," the Arizona Supreme Court observed, "is the injury to the feelings of the plaintiff, the mental anguish and distress caused" by the invasion of privacy.[188] Indeed, the notion that an invasion of privacy is a personal injury to the feelings traces back to the inception of the tort in Samuel D. Warren's and Louis D. Brandeis's *The Right to Privacy*.[189]

The same is true for all claims for electronic surveillance. The Wiretap Act and Stored Communications Act protect a user's reasonable expectations of privacy. As Justice Douglas explained: "The traditional wiretap or electronic eavesdropping device ***264** constitutes a dragnet [that] ... *intrudes upon the privacy* of those not even suspected of crime and intercepts the most intimate of conversations."[190]

Intuitively, the personal nature of electronic surveillance meshes with the experience of end-users. Electronic privacy laws protect users' interface with devices that accompany us throughout the day: the cell phones forever on our persons, the tablets by our bedsides, the laptops at our desks, the gaming consoles in the hands of our children. I do not expect that third parties will surreptitiously activate my webcam and record intimate details of my life. Nor do I expect remote intruders to intercept my Skype calls or Gmail missives. A private sphere surrounds my interface with such devices and when a third party invades that sphere, it causes an injury to the feelings. Illegal surveillance is, hence, a personal injury.

Nothing in the text of the FSIA displaces this intuitive, common law understanding of the right to privacy. First, there is no textual limitation to *bodily* injuries. While the statute distinguishes "personal injury" from property damage, it makes no distinction between injuries to the body and injuries to the feelings.[191] And that is a distinction Congress knows how to make. It did so in the Bankruptcy Code by limiting certain exemptions to damages for "personal bodily injury."[192] Aware that Congress sometimes makes this distinction, the Supreme Court has, in other contexts, construed the unrestricted term "personal injuries" to embrace physical and nonphysical harms.[193]

Second, excluding non-physical injuries would render the final clause of the tort exception entirely superfluous. Section 1605(a)(5)(B) specifically immunizes states against claims for "malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights."[194] Since these all involve nonphysical injuries, Congress would have had ***265** no reason to exclude them if such harms were not personal injuries for FSIA purposes.

In sum, at common law, a violation of privacy is an injury to the psyche. And nothing in the FSIA contradicts that traditional understanding. Courts construing the FSIA should therefore follow the common law and treat electronic privacy violations as personal injuries.

D. Discretion to Spy? Illegal Acts and the Discretionary Function Exception

Foreign sovereign defendants will invoke one final hurdle--discretionary acts immunity. The tort exception contains an important carve-out, which preserves immunity for claims "based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused."[195] The FSIA discretionary function clause was modeled on the Federal Tort Claims Act ("FTCA"), which governs suits against the United States government.[196] As a result, courts interpret the FSIA's clause in light of FTCA jurisprudence.[197]

In *United States v. Gaubert,* the Supreme Court adopted a two-step process for identifying a discretionary function under the FTCA;[198] same analysis applies to the FSIA.[199] First, the governmental conduct must involve an "element of judgment or choice" and second, that choice must involve the kind of public policy judgment the exception was designed to shield.[200] Ultimately, *Gaubert's* aim is to avoid "judicial 'second-guessing' of legislative and administrative decisions grounded in social, economic, and political policy through the medium of an action in tort."[201]

The *Gaubert* standard is easy to formulate, but hard to apply. Courts and commentators have disagreed on what exactly constitutes ***266** a discretionary function and how it should be determined.[202] But erring on the side of discretion can have harsh effects. An overbroad reading would cause the exception to swallow the rule: almost any governmental act could be characterized as being grounded in public policy, if you view it at a high enough level of abstraction.[203]

Courts should not lose sight of the obvious: a government's discretion to act is bounded by (1) legal prohibitions and (2) limited grants of jurisdictional authority. As the Supreme Court has observed, an act is not discretionary if it violates a mandatory requirement or prohibition.[204] So if the law *requires* a certain action, an official has no choice but to comply.[205] And if the law *forbids a* certain action, then an official has no discretion to break the law.[206] By the same token, if government officials are only delegated a limited jurisdiction, they have no discretion to exceed that jurisdiction.[207]

***267** Of course, between the two poles of what-is-forbidden and what-is-required lies a grey zone of discretion. This is the real province of the *Gaubert* test, for it is here that governmental decisions on the allocation of scarce resources or the prioritization of public demands are "grounded in social, economic, and political policy."[208]

Fortunately, unlawful surveillance and cyberattacks are not part of this grey zone, and their characterization is much simpler. When foreign states infiltrate U.S. computer networks they breach both limits on discretion: they violate U.S. computer misuse laws and they act without any jurisdiction to conduct surveillance in U.S. territory.

1. Criminal Law as a Check on Discretion

Courts construing the FSIA tort exception have held that a foreign state has "no discretion to commit, or to have one's officers commit, an illegal act."[209] In the influential *Letelier* decision, discussed in Part II.A., the court held that foreign states do not have a policy option to commit serious crimes such as assassination in the United States--at least not one entitled to deference under the FSIA.[210] Relying on *Letelier,* the Ninth Circuit held in *Liu v. Republic of China* that Taiwanese intelligence agents had no discretion to assassinate a dissident in California--in violation of clear U.S. and Taiwanese criminal laws.[211] Like the Ninth Circuit, the D.C. Circuit ***268** has embraced *Letelier,* noting that "case law buttresses the proposition that a criminal act cannot be discretionary."[212]

But not all illegal acts are created equal. Following *Letelier,* courts treat the illegal acts limitation not as a bright-line rule, but as a spectrum. At one extreme, criminal acts directly perpetrated by state actors are generally considered non-discretionary.[213] At the other extreme, mere complicity or negligent supervision will often be deemed a discretionary function entitled to immunity.[214] As the Ninth Circuit observed in *Risk v. Halvorsen,* not "every conceivably illegal act is outside the scope of the discretionary function exception."[215] In *Risk,* a father sued Norway and its consular officials for giving travel documents and consular assistance to the estranged mother of the plaintiff's children who then took her children to Norway in violation of a California custody order.[216] Noting that the acts of the consular officials were squarely within their functions under the Vienna Convention on Consular Relations, the court held that such acts were discretionary.[217] Of course, the illegal act of violating custody was performed by the mother, not by the Norwegian government.

Risk shows that governmental conduct is more likely to be found discretionary when it is several steps removed from actual criminal acts. Thus in *Doe v. Holy See,* the Ninth Circuit held that the discretionary function exception shielded the Holy See

from claims for the negligent supervision or retention of a priest accused of child molestation--but not from *respondeat superior* claims for the intentional tort of battery.[218] The priest--an agent of the Holy ***269** See--had no discretion to commit such abuse within the scope of his employment.[219]

Similarly, another court held that a Saudi official who recommended grants to a charity was exercising a discretionary function, even if the funds were later diverted to terrorist groups: grant-making is a classic choice "grounded in social, economic, and political policy."[220] And, as in *Risk* and *Holy See,* the governmental conduct was linked only indirectly to the criminal act.

At the far end of the spectrum, certain regulatory infractions simply are not illegal enough to be beyond the bound of discretion. When a neighborhood association sued Peru for building a chancery in D.C. that failed to comply with zoning regulations, the D.C. Circuit held that mere zoning infractions do not compare to *malum in se* offenses, and do not justify withholding immunity.[221]

But illegal wiretapping and hacking are not like zoning violations, grant recommendations, or consular assistance to violators of custody. These are computer crimes directly committed by state agents--and serious felonies under U.S. law.[222] Moreover, there is longstanding precedent that unlawful surveillance and trespass are precisely the sort of illegal acts that do not qualify as discretionary functions.

For decades, U.S. courts have recognized that governmental actors have no discretion to trespass, eavesdrop, or open mail in violation of federal law.[223] More than fifty years ago, the Supreme ***270** Court announced in *Hatahley* that wrongful trespass, in violation of federal law, was not shielded by the FTCA discretionary function clause.[224] In *Hatahley,* federal agents rounded up and slaughtered horses belonging to Native Americans on a public range, claiming they had been "abandoned" under a Utah statute, which permitted such horses to be culled.[225] The Federal Range Code, however, required federal agents to serve written notice and an order to remove livestock prior to impounding the animals.[226] Because the agents failed to give notice, the Court held that their action violated federal law and constituted actionable trespass.[227] And since the agents had no option to violate the law, they had no discretion to exercise.[228]

Following *Hatahley,* lower courts have consistently held that unlawful surveillance operations do not fall within the FTCA discretionary function clause. The warrantless interception of mail has long been held to be non-discretionary. In *Birnbaum v. United States,* the Second Circuit refused to apply the FTCA discretionary exception to the CIA's twenty-year operation of covertly opening mail of American citizens suspected of communist sympathies, holding that the CIA had no discretion to exceed the scope of its delegated authority by conducting domestic surveillance.[229] *A fortiori,* foreign intelligence agencies can have no discretion to conduct surveillance in the United States, when they have *no* delegated authority to act.

Trial courts have also refused to immunize illegal mailinterception as a discretionary function.[230] Citing *Hatahley,* the court ***271** in *Cruikshank v. United States* held that "government agents do not have the discretion to break the law."[231] As *Cruikshank* observed, giving governmental actors discretion to commit crimes is incompatible with the rule of law:

> [I]f this country has learned nothing else in the past decade, it has learned that no man, nor any man acting on behalf of our government, is above the law. The Government should not have the "discretion" to commit illegal acts whenever it pleases. In this area, there should be no policy option.[232]

Our courts have long denied this "policy option" to foreign and domestic governments. *Hatahley* and its progeny were the basis for the FSIA's "illegal act" limitation announced in *Letelier* and imposed against foreign states in *Liu*.[233] There is thus an unbroken chain of FTCA and FSIA case law that denies discretionary function immunity for clearly illegal acts. Although no court has yet to apply this line of authority to foreign state surveillance, it would be absurd to give a foreign state greater latitude to spy on U.S. citizens on U.S. soil than our own government enjoys.

2. Territorial Sovereignty as a Check on Discretion

Just as a foreign state and its agents have no discretion to commit illegal acts, they have no discretion to exceed a delegation of authority or grant of jurisdiction.[234] This is because a foreign state's authority to conduct surveillance within U.S. borders is entirely contingent on the consent of the United States.

It is axiomatic that the United States exercises exclusive territorial sovereignty within its borders. Writing in 1812, Chief Justice John Marshall observed that "[t]he jurisdiction of the nation within its own territory is necessarily exclusive and absolute" and that "[a]ll exceptions ... to the full and complete power of a nation within its own territories, must be traced up to *the consent of the* ***272** *nation itself*."[235] This consent requirement is a bedrock of customary international law. As a leading treatise notes, "police or tax investigations may not be mounted ... on the territory of another state, except under the terms of a treaty or other consent given."[236]

These international law principles do not change in cyberspace.[237] States, including the United States, continue to assert their territorial jurisdiction over cyber infrastructure and activities on their territory, and their right to "protect their cyber infrastructure against transborder interference by other States or by individuals."[238] Indeed, the Obama administration has asserted that certain acts in cyberspace may violate U.S. territorial sovereignty, including attacking or exploiting computer networks and violating privacy and civil liberties.[239]

***273** If general international law provides one constraint on foreign states' discretion to trespass on our computer networks, domestic law and bilateral treaties offer an additional check. Federal law provides a framework through which a foreign state can secure the cooperation of U.S. agencies or courts in the collection of evidence as part of criminal or tax investigations.[240] The United States has entered into numerous bilateral treaties, called Mutual Legal Assistance Treaties (MLATs), which set out duties and procedures for cross-border investigations.[241]

There is thus a mandatory channel through which foreign law enforcement and intelligence agencies must conduct investigations in U.S. computer networks-- through cooperation with U.S. agencies, pursuant to a MLAT or other bilateral agreement.[242] Further, this cooperation is subject to constitutional guarantees.[243] Giving foreign states discretion to circumvent this channel would undermine key protections of civil liberties. Federal electronic surveillance law is designed to protect people in the United States from arbitrary governmental intrusion. Yet immunizing foreign surveillance activities in U.S. computer networks would create a perverse incentive for foreign states *not* to cooperate with U.S. law enforcement. Why be bound by the Fourth Amendment and federal privacy law, when a foreign agent could simply infiltrate U.S. computer networks without fear of incurring liability?

Moreover, unauthorized cyber-surveillance does not just exceed jurisdictional limits--it also violates a "mandatory regulation."[244] Operating in the United States as an unregistered agent of a foreign government is a felony offense. Section 951 of title 18 provides criminal penalties for anyone "other than a diplomatic or ***274** consular officer or attache, [who] *acts* in the United States as an agent of a foreign government without prior notification to the Attorney General."[245]

Conducting unauthorized surveillance and intelligence gathering operations against political dissidents in the United States is precisely the type of conduct targeted by § 951--the unregistered foreign agent statute. A dual U.S.-Syrian citizen was recently convicted under this statute after he made video and audio recordings of Syrian dissidents in Washington D.C. on behalf of the *mukhabarat*--the Syrian intelligence agency.[246] Similarly, an Illinois newspaper publisher who fed the identities of Iraqi opposition members to Iraqi intelligence agencies was convicted under § 951.[247] Logic dictates that if foreign agents lack discretion to record dissident activities in the U.S. through a camcorder, then they lack discretion to record those same activities through a webcam or keylogger.[248]

In short, when foreign state agents hack into U.S. computers and surveil U.S. targets without the consent of the United States--and without respecting constitutional and statutory safeguards--they exceed their authority and have no discretion to act.[249] There is simply no latitude to exercise unlawful police powers in U.S. territory.

***275 III. PUBLIC VALUES IN THE DIGITAL DOMAIN: THE JUSTICIABILITY OF CYBER TORT CLAIMS AGAINST FOREIGN STATES**

The previous Parts have cleared the path and shown how plaintiffs can sue foreign states for surveillance and hacking committed in the United States. Federal and state laws provide a range of civil remedies, and the hurdle of immunity can be overcome. Legal doctrine, it would seem, is on the privacy plaintiffs side--but there is more at play than doctrine.

Few contemporary issues are as controversial as the rise of dragnet surveillance in cyberspace. As the Edward Snowden leaks

revealed, the United States has engaged in pervasive electronic eavesdropping at home and abroad.[250] There is much debate over the domestic and international legality of these programs--not to speak of their wisdom as public policy.[251] In March 2014, the U.N. Human Rights Committee called on the United States to ensure that its surveillance activities within and *outside* the United States comply with international privacy rights, regardless of the nationality or location of the target being surveilled.[252]

***276** Given these controversies, courts faced with electronic privacy claims against foreign states might be reluctant to reach their merits. Even if such claims do not directly implicate the legality of U.S. surveillance, they may risk exposing the United States to reciprocal treatment in the courts of foreign countries.[253] A number of questions ensue: should tort law provide protection against foreign state surveillance and cyberattacks? Should courts await further instruction from Congress? Are such claims really justiciable?[254]

Ostensibly, the concept of justiciability has been formalized in a number of discrete doctrines.[255] But as Alexander Bickel saw it, prudential judgment "resists being domesticated" and distilled into rules and standards.[256] In practice, justiciability is often a matter of judicial temperament and mood, and cases touching on foreign affairs and national security can often spoil the mood.[257] Thus recent cases challenging U.S. government surveillance in the United States and Chinese surveillance in China have been resolved on standing or ***277** political question grounds, rather than on the merits, despite the existence of fairly clear domestic and international legal standards.[258]

It is therefore worth considering in some detail why cyber tort claims against foreign sovereigns belong in the courts. This Part argues that such claims are indeed justiciable. First, the territoriality requirement of the FSIA tort exception defuses certain prudential concern, by placing the actions of foreign states *within their own borders* beyond the scope of the tort exception. Moreover, since electronic privacy claims under the FSIA invoke a clear statutory framework, they task courts with a traditional judicial function--statutory interpretation. That such claims are not political questions is clear from our long, common-law history of adjudicating governmental trespass through tort law. Finally, the fear of reciprocity does not jibe with the reality of current international law. Numerous countries deny immunity for territorial torts, meaning the United States is already substantially exposed to the risk of litigation in foreign courts.[259] Refusing to enforce the rights of U.S. residents against foreign spying will do little to alter that reality.

***278** At the outset, the FSIA's requirement that the surveillance occur within U.S. territory makes adjudication under U.S. law more appropriate. Thanks to this territorial restriction, the act of state doctrine, for example, would not apply. As traditionally formulated, that doctrine only bars our courts from adjudicating the sovereign acts of a foreign government *"done within its own territory*."[260] Courts are free, however, to "judge the legality and propriety of an act that occurred within the borders of the United States."[261] There is nothing controversial in applying U.S. law to violations of U.S. computer networks. In fact, it would be far more controversial for a court to import foreign privacy standards, which conflict with our laws and public values, to excuse foreign hacking.[262]

The territorial contours of the FSIA tort exception and the act of state doctrine are mutually exclusive. A tort must occur in U.S. territory for the FSIA tort exception to apply and in foreign territory for the act of state doctrine to apply. It is no wonder then that *Liu* and *Letelier* both rejected the act of state defense after applying the tort exception.[263] As *Letelier* recognized, giving a cross-border tort the status of an act of state would re-impose the immunity waived by the FSIA through the "back-door" of justiciability.[264]

Nor are such claims necessarily political questions. Not "every case or controversy which touches foreign relations lies beyond ***279** judicial cognizance."[265] Indeed, recent Supreme Court jurisprudence suggests that modern political questions only arise in two circumstances.[266] First, courts will not decide cases arising from "a textually demonstrable constitutional commitment of the issue to a coordinate political department."[267] Second, courts will not decide cases that present "a lack of judicially discoverable and manageable standards."[268]

Neither rationale would bar a privacy claim brought under the FSIA because such claims turn on statutory interpretation--a quintessential judicial function, textually committed to the Article III courts. Indeed, the Supreme Court has *never* found a political question arising from a statutory violation.[269] And after the Court's 2012 decision in *Zivotofsky ex rel. Zivotofsky v. Clinton,* it is doubtful that a statutory claim could *ever* present a political question.[270] In *Zivotofsky,* the Supreme Court reversed a lower court ruling that the political question doctrine barred petitioners' request to list their child's place of birth as

"Jerusalem, Israel" in official documents, pursuant to the Foreign Relations Authorization Act.[271] The plaintiff, the Court reasoned, sought to vindicate a statutory right, not to seek judicial recognition of Jerusalem as the capital of Israel.[272] This raised no political question for two reasons. First, the adjudication of a statutory right is committed to the courts, not to the Executive.[273] Second, where a statute supplies a rule of decision, there is no "lack of judicially discoverable" standards. Construing the meaning of a ***280** statute and reviewing its constitutionality is "a familiar judicial exercise."[274] This line of reasoning has a broad impact. Although *Zivotofsky* was decided on a narrow set of facts, its rationale applies with equal force to *any* claim that vindicates a statutory right.[275]

Under that rationale, a wiretapping or computer trespass claim brought under the FSIA cannot be characterized as a political question. The ECPA and CFAA set out clear standards to ascertain liability for an interception or computer trespass. Determining the scope of liability under these laws is, as we saw above, a traditional exercise in statutory construction. As for immunity, Congress delegated this inquiry to the judicial branch when it codified common law and international law norms in the FSIA.[276] The courts have consistently construed the text of the FSIA to determine the scope of immunity--regardless of the impact on foreign relations.[277] Applying the FSIA to privacy claims is no different.

History suggests that surveillance claims are legal, not political questions. Using tort law to guard against governmental eavesdropping and trespassory searches is deeply rooted in Anglo-American tradition. For more than two hundred years, American and British courts have 'second-guessed' government surveillance operations "through the medium of an action in tort."[278] *Entick v. Carrington,* a 1765 case tried before the King's Bench, is widely considered to have laid the foundation for the Fourth Amendment's protection against illegal searches and seizures.[279] And it did so through tort. At eighteenth-century common law, a constable who searched a home without a valid warrant was strictly liable in trespass.[280] In *Entick,* King George Ill's messengers were given a warrant to enter the home of John Entick and search his papers, ***281** seeking to identify the author of an allegedly libelous article.[281] Entick sued for trespass.[282] Finding that no common-law rule justified the general warrant to seize Entick's books and papers, Lord Campbell, Chief Justice of the Court of Common Pleas, held that the King's messengers were liable in tort.[283]

Entick was just one of six English court decisions handed down in the mid-eighteenth century that used tort law as a check on abusive searches and seizures.[284] Known as the "General Warrants" cases, all six affairs involved the Crown's effort to crack down on *lèse majesté* and arrest the authors of allegedly libelous publications.[285] In all six cases, tort actions were used to challenge the practice of general warrants.[286] In the words of one commentator, these precedents "established the rights of privacy that have been treasured in American and English law ...."[287]

Just as tort law was critical to the English constitution, it remains critical to the Supreme Court's understanding of the Fourth Amendment and the common law of privacy.[288] Tort suits continue to serve as an essential check on unlawful surveillance.[289]

Given this long history, wiretapping and computer trespass are precisely the types of tortious acts that are susceptible to judicial review. Today's cyber trespasses are the modern equivalent of the abusive searches of King George Ill's. Only now, the globally-networked nature of computer systems means that foreign powers can trench on civil liberties within our borders. But the ***282** remedies are the same: Courts need only apply old laws to new technologies.

This is not to say that electronic privacy suits against foreign sovereigns raise no questions of international law and foreign affairs. One vital concern in any suit against a foreign government is reciprocity: will the United States or its officials receive treatment in kind? Indeed, reciprocity was foremost in the mind of one of the FSIA's principal drafters, Bruno Ristau, who testified to the House Judiciary Committee that:

> We would like, based on our experience as a litigant abroad, to subsume to the jurisdiction of our domestic courts foreign governments and foreign entities who engage in certain activities on our territory *to the same extent that the U.S. government is already at the present time subject to the jurisdiction of foreign courts, when it engages in certain activities on their soil*.
>
> ...

> [W]e would like to afford our local citizens and entities who deal with foreign governments in the United States effective redress through the instrumentality of our courts.[290]

To grasp the reciprocity concerns underpinning the FSIA, courts should consider the current international landscape of sovereign immunity. The United States is not alone in denying immunity for torts occurring within the forum state's borders.[291] The territorial tort principle is enshrined in national legislation around the world. For example, the foreign state immunity statutes of Argentina,[292] Australia,[293] Canada,[294] Israel,[295] Japan,[296] Singapore,[297] ***283** South Africa,[298] and the United Kingdom[299] all deny immunity for certain torts occurring in their territories on grounds similar, if not always identical, to those of the FSIA. The upshot is that the United States is already exposed to potential tort liability in foreign countries for wrongs committed in their territory--and in their cyber infrastructure. Indeed, on June 4, 2014, in the fall-out of the Snowden revelations, German Federal Prosecutor Harald Range announced the opening of an investigation into the wiretapping of German Chancellor Angela Merkel by U.S. agents.[300] Subjecting foreign states to our courts, just as the United States is subjected to theirs, is thus a matter of parity.

Finally, as a policy matter, tort litigation may be more desirable than the alternatives. Electronic privacy suits provide a peaceful channel for dispute resolution, in contrast to other proposed responses to trans-border cyberattacks. The White House's *International Strategy for Cyberspace* asserts the right to use all necessary means to counter intrusions into U.S. cyber infrastructure, including armed force.[301] In response to the Sony hack, President Obama imposed sanctions on a number of North Korean governmental entities and individuals, citing "North Korea's attack that aimed to create destructive financial effects on a U.S. company and to threaten artists and other individuals with the goal of restricting their right to free expression."[302]

***284** This type of tit-for-tat diplomacy can easily escalate. Commentators have suggested that states could engage in limited retaliation against foreign state-sponsors of cyberattacks under the international law of countermeasures-- a form of self-help for injured states.[303] Jeremy and Ariel Rabkin have even proposed reviving the practice of issuing "letters of marque"--commissions that authorized eighteenth century privateers to raid enemy-flagged vessels--to private U.S. actors.[304] This would legitimate reprisals against the computers of foreign hackers, but from a rule of law standpoint, are plaintiffs not preferable to privateers?

Of course, criminal prosecutions are another possibility. On May 19, 2014, a federal grand jury returned an indictment against five Chinese military officials for allegedly engaging in economic espionage against U.S. businesses through computer hacking.[305] But as a practical matter, the Chinese government is unlikely to extradite the defendants, so the indictment functions more as a diplomatic shot across the bow. This would be so for most true bills: obtaining jurisdiction over individual foreign officials is rarely an option.

Prosecuting a foreign state poses other problems. The *criminal* liability of foreign governmental entities is a novel issue and would hinge on the specific statute in question.[306] At least one court has held that governmental entities--in this case domestic--cannot be prosecuted under the Wiretap Act.[307] In contrast, the Computer ***285** Fraud and Abuse Act does contemplate criminal liability for such entities, since "any person"--a term that includes governmental entities--can be "convicted of a violation."[308] Even so, civil liability is less conceptually difficult and, perhaps, less provocative. A civil suit packs less normative punch than a criminal indictment. In the sensitive area of foreign affairs, that can be a virtue.

Given these difficulties, tort remedies for foreign state-sponsored cyberattacks are more effective and less incendiary than self-help vigilantism, criminal prosecution, or armed escalation. They also provide a measure of redress to victims, while restoring public confidence in the rule of law.

Money damages are available to a plaintiff who overcomes FSIA immunity,[309] though recovery will be limited to a compensatory award, since the. FSIA exempts foreign sovereigns from punitive damages.[310] Yet despite this limitation, the statutory and common law actions for computer trespass and electronic privacy can still put a considerable price tag on unlawful surveillance. The Wiretap Act, for example, provides for statutory damages, recognizing the fact that the injury caused by an invasion of privacy can be hard to quantify.[311] In cases of prolonged surveillance, these sums could potentially deter violations. An even stronger deterrent is the expressive power of tort liability. Having a court declare that a foreign state has violated U.S. law by hacking into U.S. computers would send a powerful signal that citizens' digital rights are taken

seriously.

Upon closer inspection, electronic privacy suits against foreign sovereigns are less controversial than they first appear. They do not ask courts to make unmoored policy decisions. Rather, they seek application of the rules for liability and immunity that Congress put in place--a task delegated to the courts. If these suits ultimately strain our foreign relations, it is up to Congress to amend our privacy and immunity laws, not the courts.

***286 CONCLUSION**

Surveillance powers are often abused. And that abuse has often been the source of dramatic social change. From King George Ill's general warrants to the recent uprisings in the Middle East, the shock of living under the gaze of government can spur people to assert their basic rights to think and speak freely. Citizens facing surveillance by their own government have at least some recourse: they can use the democratic process, invoke the constitution, or--as in the Arab Spring--take to the streets.[312]

When the spy is a foreign power, though, these routes are closed. A journalist in New York cannot vote a less invasive regime into power in China. An asylee from Ethiopia can hardly lodge a constitutional complaint in Addis Ababa for the hijacking of his webcam in Washington.

What these victims of foreign-state hackers *can* do is go to the courts of the United States and invoke their rights under statute and common law. In 1976, Congress opened the courthouse doors to those harmed by the acts of a foreign state inside U.S. borders. In enacting the FSIA, Congress struck a new balance between the rights of individuals and the prerequisites of sovereignty. Absolute immunity is a thing of the past, a "relic of the doctrine of the divine right of kings," in the words of Justice Robert H. Jackson.[313] When foreign states reach into our borders--and our computers--they subject themselves to the jurisdiction of our courts.

This Article has shown a path for the electronic privacy plaintiff. From the computer misuse statutes to common law torts, the hacked can assert a number of rights against the hackers. In a narrow set of cases, immunity can be overcome. When a foreign state intrudes upon computer networks in the United States, in violation of U.S. law, the FSIA is no barrier to suit.

Such claims are not just in the private interest of the plaintiffs--they are in the interest of the public. Cyber tort suits are ***287** more than a redistributive mechanism: they can express public values and enforce limits on sovereign power in the digital domain. Tort law reined in governmental excess in eighteenth century England--and it can help extend the rule of law into cyberspace today.

Footnotes	
a1	Staff Attorney, Center for Justice and Accountability; J.D., George Washington University Law School; B.A., McGill University. The author is a consulting attorney with the Electronic Frontier Foundation. The views expressed herein are not intended to reflect the official positions of the Center for Justice and Accountability or the Electronic Frontier Foundation.
1	Eric Grosse, *Security warnings for suspected state-sponsored attacks,* Google Online Security Blog (June 5, 2012, 12:04 PM), http:// googleonlinesecurity.blogspot.com/2012/06/security-warnings-for-suspected-state.html.
2	Jeremy Wagstaff, *Journalists, media under attack from hackers: Google researchers,* Reuters (Mar. 28, 2014 5:48 AM), http:// www.reuters.com/article/2014/03/28/us-media-cybercrime-idUSBREA2R0EU20140328.
3	Nicole Perlroth, *Hackers in China Attacked the Times for Last 4 Months;* N.Y. Times, Jan. 30, 2013, http:// www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0.
4	*Id. See also* Mandiant, APT1: Exposing One of China's Cyber Espionage Units 21, 22 (Feb. 18, 2013), *available at* http:// www.mandiant.com/apt1 (identifying 115 entities and organizations in the United States targeted by malware attacks and data exfiltration attributed to a unit of the Chinese military).

5	*NY Times says Chinese hacked paper's computers,* Yahoo News (Jan. 30, 2013, 1:55 PM), http://news.yahoo.com/ny-times-says-chinese-hacked-papers-computers-070948109--finance.html; Julie Moos, *Chinese hackers infiltrate the New York Times, Wall Street Journal,* Poynter (Jan. 31, 2013), http:// www.poynter.org/latest-news/mediawire/202400/chinese-hackers-infiltrate-new-york-times-bloomberg/; Andrew Beaujon, *Washington Post confirms it was hacked by Chinese, too,* Poynter (Feb. 1, 2013), http://www.poynter.org/latest-news/mediawire/202629/why-havent-chinese-hackers-struck-the-washingtonpost/.
6	*See* George C. Thomas III, *Stumbling Toward History: The Framers' Search and Seizure World,* 43 Tex. Tech. L. Rev. 199, 210-14 (2010).
7	*See* Larry M. Wortzel, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology,* Testimony Before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations (July 9, 2013); Josh Rogin, *NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History',* Foreign Policy: The Cable (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.
8	Press Release, FBI National Press Office, Update on Sony Investigation (Dec. 19, 2014), *available at* http:// www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
9	*Id.*
10	David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony,* N.Y. Times, Dec. 17, 2014, http:// www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0.
11	*See* Duncan B. Hollis, *An e-SOS for Cyberspace,* 52 Harv. Int'l L.J. 374, 399 (2011) ("Attribution can occur, but usually does so via secondary intelligence, dumb mistakes, or some admission of responsibility in lieu of tracing attacks back to their original source."); *see also* David D. Clark and Susan Landau, *Untangling Attribution,* 2 Harv. Nat'l Sec. J. 1, 21 (2011) ("Evidence of on-line identity, however robust technically, may be less compelling than evidence gathered from carrying out search warrants and following the money. Packet-level attribution may aid an investigation, but our world still demands that the real evidence come from the physical world.").
12	*See* Hollis, *supra* note 11, at 399 (noting that cyberattackers using botnets--a network of surreptitiously hijacked and automated computers--can raise obstacles between the commanding and slave computers and "launder" data packets to mask an attack's origins).
13	*Id.*
14	Ryan Faughnder & Saba Hamedy, *Sony insider - not North Korea - likely involved in hack, experts say,* L.A. Times (Dec. 14, 2014), http:// www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-inside-job-not-north-korea-20141231-story.html.
15	Evan Perez, et al., *Obama: Sony 'made a mistake,'* CNN (Dec. 19, 2014), http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/.
16	Craig Timberg, *Foreign regimes use spyware against journalists, even in U.S.,* Wash. Post (Feb. 12, 2014), http:// www.washingtonpost.com/business/technology/foreign-regimes-use-spyware-against-joumalists-even-in-us/2014/02/12/9501a20e-9043-lle3-84el-27626c5ef5fb_ story.html; Bill Marczak et al., *Hacking Team and the Targeting of Ethiopian Journalists,* The Citizen Lab of the Munk School of Global Affairs, Univ. of Toronto (Feb. 12, 2014), https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/.
17	Eva Galperin & Morgan Marquis-Boire, *Fake YouTube Site Targets Syrian Activists with Malware,* Electronic Frontier Foundation (Mar. 15, 2012), https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware.
18	Eva Galperin & Morgan Marquis-Boire, *Vietnamese Malware Gets Very Personal,* Electronic Frontier Foundation (Jan. 19, 2014), https:// www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal.

19	Nicole Perlroth, *Software Meant to Fight Crime Is Used to Spy on Dissidents,* N.Y. Times, Aug. 31, 2012, at Al.
20	*See* Marczak et al., *supra* note 16; Morgan Marquis-Boire et al., Citizen Lab and Canada Centre for Global Security Studies, Univ. of Toronto, For Their Eyes Only: The Commercialization of Digital Spying 6-26 (2013), *available at* https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf (analyzing samples of the FinFisher spyware suite recovered from the computers of pro-democracy activists in Bahrain).
21	Marquis-Boire et al., *supra* note 20, at 16, 19 (discussing forensic analysis of hidden directory installed by FinSpy on a targeted computer hard drive that included "keylogger data, audio from Skype calls, passwords and more").
22	*See id.* at 79 (discussing promotional materials for the Remote Control System spyware suite touting the following features, among others: web browsing, Keystrokes, Remote Audio Spy [sic], and Camera Snapshots).
23	Dan Blumenthal, *How to Win a Cyberwar with China,* Foreign Policy (Feb. 28, 2013), http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_ cyberwar_with_china (proposing a cyberattack exception to Foreign Sovereign Immunities Act).
24	Andrew Zajac, *Ethiopian Government Accused of Spying on U.S. Citizen,* Bloomberg News (Mar. 10, 2014, 5:31 PM), http://www.bloomberg.com/news/2014-03-10/ethiopian-government-accused-of-spying-on-u-s-citizen.html.
25	*See* Pub. L. No. 94-583, 90 Stat. 2891 (1976) (codified at 28 U.S.C. §§ 1330, 1332, 1391(f), 1441(d), 1602-11 (2012)).
26	The Author is a consulting attorney with the Electronic Frontier Foundation in *Doe, a.k.a. Kidane v. Federal Democratic Republic of Ethiopia,* No. l:14-cv-00372 (D.D.C.), the first case to test this Article's legal theory.
27	28 U.S.C. § 1605(a)(5) (2008).
28	Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, Oct. 21, 1986, 100 Stat. 1848.
29	Originally enacted as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190-92, and codified at 18 U.S.C. § 1030, the CFAA has been modified and significantly expanded five times. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act,* 94 Minn. L. Rev. 1561, 1561 (2010) [hereinafter Kerr, *Vagueness Challenges]* (discussing the scope and development of the Computer Fraud and Abuse Act).
30	18 U.S.C. §§ 2510-22 (2012). The Wiretap Act was first introduced as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, § 802, 82 Stat. 212 (1968).
31	18 U.S.C. §§ 2701-11 (2012), originally enacted as Pub. L. No. 99-508, Title II, § 201[a], 100 Stat. 1860 (1986).
32	18 U.S.C. §§ 3121-27 (2012), originally enacted as Pub. L. No. 99-508, Title III, § 301(a), 100 Stat. 1868 (1986).
33	The Pen Register Act is not relevant for present purposes, since it does not provide a private right of action.
34	The Act provides that, "Except as otherwise specifically provided in this chapter[,] any person who--intentionally intercepts, endeavors to intercept, or procures any other person to intercept ... any wire, oral, or electronic communication ... shall be punished ... or shall be subject to suit." 18 U.S.C. § 2511(1) (2012). The Act includes a court order exception, § 2511(2)(a), party consent exception, § 2511(2)(c), and a limited service provider exception, § 2511(2)(a).
35	18 U.S.C. §2511(1) (2012).
36	United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); *accord* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2001); *In re* Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).

37	18 U.S.C. § 2510(12) (2012) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce ...."). Because the definition requires a nexus to commerce, some courts have found that signals sent between computer external hardware *(e.g.*, a keyboard or mouse) and a terminal port are not "electronic communications," since they do not move through interstate or foreign commerce. *See, e.g.,* United States v. Barrington, 648 F.3d 1178, 1202 (11th Cir. 2011) (noting that "use of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce"); United States v. Ropp, 347 F. Supp. 2d 831, 837-38 (CD. Cal. 2004) (holding that the Wiretap Act's definition of electronic communications applies only to data being transmitted beyond a local computer through a system that affects interstate commerce).
38	*See, e.g.,* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (holding that Wiretap Act applies to the interception of packet switched phone calls and e-mails); United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) (holding that "'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications" and hence interception of e-mail in such storage violates the Act); Klumb v. Goan, 884 F. Supp. 2d 644, 661 (E.D. Tenn. 2012) ("[U]nder the router switching analysis, a wiretap occurs when spyware automatically routes a copy of an email, which is sent through the internet, back through the internet to a third party's email address when the intended recipient opens the email for the first time.").
39	18 U.S.C. § 2520(a) (2012).
40	Stored Communications Act, 18 U.S.C. §§ 2701-12 (2012). For background on the SCA, *see* Orin S. Kerr, A *User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208, 1213-14 (2004).
41	18 U.S.C. § 2701(a)(1) (2012).
42	18 U.S.C. § 2707 (2012).
43	*See, e.g., In re* Doubleclick, Inc., 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001) (holding that cookies placed on plaintiff's personal computer are not covered by the SCA, since the plaintiff is a user--not a provider--of electronic communications services). For statutory definitions of these terms see 18 U.S.C. § 2510 (2012).
44	*See* Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *5-6 (E.D. Mich. Feb. 6, 2008) (denying summary judgment and holding that the SCA applies to a husband who used a keylogger to obtain the password to his estranged wife's e-mail account and then gained unauthorized access to messages on Yahoo servers).
45	18 U.S.C. § 1030(a)(2)(C) (2012). Overall, the CFAA criminalizes seven activities: obtaining national security information, compromising confidentiality, trespassing in a federal government computer, accessing to defraud and obtain value, damaging a computer or information, trafficking in passwords, and threatening to damage a computer, as well as attempts or conspiracies to commit these offenses. 18 U.S.C. § 1030(a) (2012).
46	The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8) (2012). "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(ll) (2012).
47	The § 1030(c)(4)(A)(i) factors include: (I) loss during a one-year period aggregating at least $5,000 in value; (II) modification or impairment of medical care; (III) physical injury; (IV) a threat to public health or safety; (V) damage to a computer used by the U.S. government for justice, national defense, or national security; or (VI) damage to ten or more protected computers during any one-year period. *See* 18 U.S.C. § 1030(c)(4)(A)(i).
48	18 U.S.C. § 1030(e)(2)(B); *see also* Kerr, *Vagueness Challenges, supra* note 29, at 1561 (noting this statute "potentially regulates every use of every computer in the United States and even many millions of computers abroad.").

49	*See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 N.Y.U. L. Rev. 1596, 1624--40 (2003) (surveying difficulties in interpreting the CFAA's terms).
50	*Compare* United States v. Nosal, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc) (holding that the CFAA applies only to access-restrictions, not to an employer or owner's use-restrictions), *with* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that an employee accessing Social Security Administration records for non-business use had exceeded authorized access).
51	S. Rep. No. 357, 104th Cong., 2d Sess., at 4-5 (1996) (discussing hacking of Air Force and Harvard University facilities by British and Argentinian hackers).
52	*See, e.g.,* PQ Labs, Inc. v. Yang Qi, 12-0450 CW, 2014 WL 334453, at *9-10 (N.D. Cal. Jan. 29, 2014) (holding that a CFAA claim survived a motion for summary judgment where defendants had allegedly obtained unauthorized access to a computer network via "phishing" e-mails that tricked recipients into entering log-in credentials).
53	*See, e.g.,* Becker v. Toca, No. CIV. A. 07-7202, 2008 WL 4443050, at *1, *5 (E.D. La. Sept. 26, 2008) (denying motion to dismiss Wiretap Act claims where a husband used "Trojan Horse" software on his wife's computer to intercept e-mails and steal passwords).
54	*See, e.g.,* Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1298, 1305, 1322-24 (S.D. Fla. 2003) (entering judgment for plaintiff for a CFAA claim based on "IP spoofing," which is "forging an IP address so that when a person receives a data packet or communication they believe it is coming from somewhere else"), *aff'd in part, rev'd in part by* 138 Fed. Appx. 297 (11th Cir. Mar. 31, 2005).
55	*See, e.g.,* United States v. Ivanov, 175 F. Supp. 2d. 367, 368, 374-75 (D. Conn. 2001) (denying defendant's motion to dismiss indictment on CFAA charges, holding that surreptitiously obtaining and using a system administrator's root password to manipulate data would, if proven, violate the CFAA).
56	Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193 (1890).
57	Paul M. Schwartz, *Preemption and Privacy,* 118 Yale L. J. 902, 907 (2009).
58	Restatement (Second) of Torts § 652B (1977).
59	*See, e.g.,* Vurimindi v. Fuqua Sch. of Bus., 435 F. App'x 129, 136 (3d Cir. 2011) (finding a cognizable privacy claim where a keylogger was used to obtain bank information); Toomer v. Garrett, 155 N.C. App. 462, 479-80, 574 S.E.2d 76, 90 (2002) (stating that cognizable intrusions include "eavesdropping by wiretapping or microphones, ... unauthorized prying into a bank account, and opening personal mail ....") (internal quotations omitted).
60	*See, e.g.,* Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1230 (N.D. Ill. 2005) (recognizing trespass to chattels action for unauthorized installation of spyware). A trespass to chattel is the "intentional interference with the possession of personal property [that] proximately cause [s] injury." eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000). *See also* Restatement (Second) of Torts § 217 *et seq.* ("A trespass to a chattel may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another.").
61	Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1347 (Sup. Ct. Cal. 2003); *see also* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (holding, in a suit involving unsolicited spam e-mail, that the element of actual harm could be established by the fact that "multitudinous electronic mailings demand the disk space and drain the processing power of plaintiffs computer equipment," and hence diminish its value to the owner).
62	*See, e.g.,* Inventory Locator Serv., LLC v. Partsbase, Inc., No. 02-2695 *MAN,* 2005 WL 2179185, at *12 (W.D. Tenn. Sept. 6, 2005) (noting that Florida "does not recognize a cause of action for trespass to chattels in cyberspace").

63	*See generally* Schwartz, *Preemption and Privacy, supra* note 57, at 916-18 (surveying state innovations in privacy, surveillance, and consumer protection law). A full examination of state electronic privacy laws is beyond the scope of this Article.
64	Cal. Bus. & Prof. Code §§ 22948.2-22948.3.
65	*See, e.g.,* Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code § 22947.3 (providing for no express enforcement provisions).
66	*See* Schwartz, *Preemption and Privacy, supra* note 57, at 919--21 (discussing risk of federal legislation setting a "ceiling" for privacy norms that could preempt state privacy protections). In addition to the conflict or field preemption risks discussed by Schwartz, litigation over state-sponsored cyberattacks could raise additional questions of foreign affairs preemption. *See generally* Jack Goldsmith, *Statutory Foreign Affairs Preemption,* 2000 Sup. Ct. Rev. 175, 202-08 (2001) (mapping preemption doctrines). Because this Article focuses primarily on federal claims, however, a preemption analysis is best left for another day.
67	28 U.S.C. § 1606 (2012) (emphasis added).
68	First Nat'l City Bank v. Banco Para El Comercio Exterior de Cuba, 462 U.S. 611, 622 n.11 (1983).
69	Estate of Heiser v. Islamic Republic of Iran, 466 F. Supp. 2d 229, 265 (D.D.C. 2006) (addressing causes of action under the state sponsors of terrorism exception, 28 U.S.C. § 1605(a)(7)); *see, e.g.,* Pescatore v. Pan Am. World Airways, Inc., 97 F.3d 1, 12 (2d Cir. 1996) ("[T]he FSIA ... operates as a 'pass-through' to state law principles."); Holland v. Islamic Republic of Iran, 496 F. Supp. 2d 1, 15 (D.D.C. 2005) ("Section 1606 ... is a mere pass-through to causes of action that would exist against private individuals."); Dammarell v. Islamic Republic of Iran, No. CIV.A. 01-2224JDB, 2005 WL 756090, at *8 (D.D.C. Mar. 29, 2005) ("[W]hen section 1605 lifts the sovereign immunity of a foreign state, Section 1606 allows a plaintiff to bring any claim against the foreign defendant that the plaintiff could have brought in like circumstances were the defendant a private individual."); Lord Day & Lord v. Socialist Republic of Vietnam, 134 F. Supp. 2d 549, 561 (S.D.N.Y. 2001) (construing the FSIA as a jurisdictional pass-through for state law).
70	*See, e.g.,* Barkanic v. Gen. Admin, of Civil Aviation of the People's Republic of China, 923 F.2d 957, 960 (2d Cir. 1991) (holding that § 1606 of the FSIA requires the application of New York choice of law rules because such rules would have governed "this wrongful death action if the parties before it were all private individuals").
71	*See* Southway v. Cent. Bank of Nigeria, 198 F.3d 1210, 1215-16 (10th Cir. 1999) (holding that FSIA gives district courts subject-matter jurisdiction over civil RICO claims against foreign states). *See also* Mukaddam v. Permanent Mission of Saudi Arabia to the United Nations, 111 F. Supp. 2d 457, 470 (S.D.N.Y. 2000) (holding that Title VII applies to foreign states through Section 1606). *But see* Holland v. Islamic Republic of Iran, 496 F. Supp. 2d 1, 16 (D.D.C. 2005) (holding that statutes of general application can pass-through § 1606 and apply to foreign states, but those with an expressly limited class of defendants cannot).
72	H. Rep. No. 94-1487, at 22 (1976), *reprinted in* U.S.C.C.A.N. 6604, 6621. Identical language was included in the Senate Report. S. Rep. No. 94-1310, at 22S. Rep. No. 94-1310, at 22 (1976).
73	Pub. L. No. 102-256, 106 Stat. 73 (codified at 28 U.S.C. § 1350).
74	*See, e.g.,* Holland v. Islamic Republic of Iran, 496 F. Supp. 2d 1, 17-18 (D.D.C. 2005) (holding that the TVPA by its terms applies only against individual defendants and hence cannot be applied against states through § 1606); Dammarell v. Islamic Republic of Iran, No. CIV.A. 01-2224JDB, 2005 WL 756090, at *31 (D.D.C. Mar. 29, 2005). To overcome this strong evidence of intent, [to limit the TVPA's scope to individual officials] the Court would require something more than the textual gymnastics of reading a 1996 statute (section 1605(a)(7)) as operating through a 1976 statute (Section 1606) to expand a 1992 cause of action (the TVPA) to the states.
75	*Holland,* 496 F. Supp. at 17-18; *Dammarell,* 2005 WL 756090, at *31.

76	S. Rep. No. 102-249, at 7 (1991).
77	Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (1968).
78	*Id.* § 2511.
79	*Id.* § 2520.
80	*Id.* § 2510.
81	Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1866 (1986).
82	*Id.* § 101(c)(A).
83	*Id.* § 103.
84	*Id.* § 201.
85	*Id.* § 201.
86	*Id.* § 101 (omitting a definition of "entity" for Wiretap Act purposes), § 201 (stating in the inserted Section 2710 of Title 18 that the Wiretap Act's definitions, 18 U.S.C. § 2510, apply to the Stored Communications Act as well).
87	Adams v. City of Battle Creek, 250 F.3d 980, 985 (6th Cir. 2001).
88	S. Rep. 99-541, at 43 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3597.
89	USA PATRIOT Act, § 223, 115 Stat. 293, 384 (2011).
90	18 U.S.C. § 2520(a) (2012); 18 U.S.C. § 2707 (2012).
91	*See Adams,* 250 F.3d at 985 (recognizing government liability under Wiretap Act and SCA); Organization JD Ltda. v. United States Dep" of Justice, 18 F.3d 91, 94-95 (2d Cir. 1994) (recognizing government liability in SCA); Garza v. Bexar Metro. Water Dist., 639 F. Supp. 2d 770, 773-74 (W.D. Tex. 2009); Conner v. Tate, 130 F. Supp. 2d 1370, 1374-75 (N.D. Ga. 2001) (same); Dorris v. Absher, 959 F. Supp. 813, 819-20 (M.D. Tenn. 1997) (same), aff'd in part on other grounds and rev'd in part, 179 F.3d 420 (6th Cir. 1999) (claims against county were settled and not addressed on appeal); PBA Local No. 38 v. Woodbridge Police Dep't, 832 F. Supp. 808, 822-23 (D.N.J. 1993).
92	*Adams,* 250 F.3d at 985.
93	*Organizacion JD Ltda.,* 18 F.3d at 94.
94	*See* Antonin Scalia & Bryan A. Garner, Reading Law: The Interpretation of Legal Texts 252 (2012).
95	*See Conner,* 130 F. Supp. 2d at 1373-74 (noting that although "a governmental entity ... could not be prosecuted criminally for a violation of the Wiretap Act ... [t]he section of the Wiretap Act which authorizes civil damages leads to a different conclusion.").
96	Seitz v. City of Elgin, 719 F.3d 654, 657 (7th Cir. 2013); Franklin v. City of Chicago Police Dep't, 175 F. App'x 740, 741-42 (7th Cir. 2005); Abbott v. Vill. Of Winthrop Harbor, 205 F.3d 976, 980-81 (7th Cir. 2000); Amati v. City of Woodstock, 176 F. 3d 952, 956 (7th Cir. 1999) ("Title III [the Wiretap Act] does not allow for suits against municipalities.").

97	*Seitz,* 719 F.3d at 658.
98	*Id.* at 656-58.
99	*Id.*
100	*Id.*
101	*See, e.g.,* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 107(b), 100 Stat. 1866 (1986) (noting the ECPA does not affect procedures approved by the Attorney General to intercept communications transmitted by foreign powers).
102	H.R. Rep. No. 99-647, at 19-20H.R. Rep. No. 99-647, at 19-20 (1986).
103	S. Rep. No. 99-541 (1986); H.R. Rep. No. 99-647H.R. Rep. No. 99-647 (1986).
104	See *generally* Scalia & Garner, *supra* note 94 (cataloguing accepted canons of statutory construction).
105	*See* Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010) (noting the "longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'") (quoting EEOC v. Arabian American Oil Co., 499 U.S. 244, 248 (1991)).
106	On this point, *see* the House Report, which clarifies that the ECPA only regulates the interception of communications "conducted within the territorial United States." H.R. Rep. No. 99-647, at 32H.R. Rep. No. 99-647, at 32 (1986).
107	Petteys v. Butler, 367 F.2d 528, 538 (8th Cir. 1966) (Blackmun, J., dissenting).
108	18 U.S.C. § 1030(0(1) (2012).
109	18 U.S.C. § 1030(e)(12) (2012).
110	18 U.S.C. § 1030(e)(9) (2012).
111	Indictment, United States v. Dong, No. 14-118 (W.D. Pa. May 19, 2014), *available at* http:// www.justice.gov/iso/opa/ resources/512201451913235846194 9.pdf.
112	*See, e.g.,* Harrison v. Republic of Sudan, 882 F. Supp. 2d 23, 46, 47-51 (D.D.C. 2012) (awarding damages for sailors' claims of, *inter alia,* assault and battery arising from a terrorist attack on a Navy vessel); Ben-Rafael v. Islamic Republic of Iran, 540 F. Supp. 2d 39, 57-59 (D.D.C. 2008) (awarding damages for wrongful death and intentional infliction of emotional distress claims arising from bombing of Israeli embassy in Buenos Aires).
113	*See, e.g.,* Doe v. Holy See, 557 F.3d 1066, 1083 (9th Cir. 2009) (lifting Holy See's immunity from *respondeat superior* claims based on a priest's sexual battery under 28 U.S.C. § 1605(a)(5) (2012)).
114	*See, e.g.,* USAA Cas. Ins. Co. v. Permanent Mission of Republic of Namibia, 681 F.3d 103, 109-10 (2d Cir. 2012) (holding that Namibian mission was amenable to negligence action for failing to maintain structural integrity of building walls).
115	*See, e.g.,* Joseph v. Office of Consulate Gen. of Nigeria, 830 F.2d 1018, 1027 (9th Cir. 1987) (holding that a landlord's tort actions for trespass, conversion, and waste are actionable against Nigeria and its Consulate under 28 U.S.C. § 1605(a)(5) (2012)).

116	28 U.S.C. § 1604 (2012); Saudi Arabia v. Nelson, 507 U.S. 349, 355 (1993).
117	28 U.S.C. § 1604 (2012) ("Subject to existing international agreements ... a foreign state shall be immune from the jurisdiction of the courts of the United States and of the States ....").
118	28 U.S.C. § 1603 (2012).
119	Samantar v. Yousuf, 560 U.S. 305, 325-26 (2010) (holding that FSIA did not displace common law regime governing foreign official immunity).
120	28 U.S.C. §§ 1605-07 (2012). The exceptions include: (1) waiver, § 1605(a)(1); (2) commercial activities, (a)(2); (3) takings, (a)(3); (4) property rights, (a)(4); (5) non-commercial torts in U.S. territory, (a)(5); (6) arbitration, (a)(6); and state sponsors of terrorism, § 1605A.
121	28 U.S.C. § 1330(b) (2012) (governing personal jurisdiction); 28 U.S.C. § 1608 (2012) (governing service of process).
122	28 U.S.C. § 1330(a) (2012).
123	Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 434 (1989).
124	28 U.S.C. § 1605(a)(5) (2012).
125	This Article's focus is on state-sponsored cyberattacks that are not related to commercial activities. There may well be incidents of economic espionage where hacking is a commercial pursuit. While such claims might be viable under the § 1605(a)(2) commercial activities exception, their commercial nature would preclude application of the § 1605(a)(5) tort exception.
126	*See* Youming Jin v. Ministry of State Sec., 475 F. Supp. 2d 54, 63-64 (D.D.C. 2007) (discussing how the tort exception is to be applied by a court).
127	H.R. Rep. No. 94-1487, at 20-21 (1976), *reprinted in* 1976 U.S.C.C.A.N. 6611-12 (emphasis added).
128	MacArthur Area Citizens Ass'n v. Republic of Peru, 809 F.2d 918, 921 (D.C. Cir. 1987), *modified,* 823 F.2d 606 (D.C. Cir. 1987); *accord In re* Terrorist Attacks on Sept. 11, 2001, 538 F.3d 71, 87 (2d Cir. 2008) (citing MacArthur Area Citizens Ass'n, 809 F.2d at 921); Fagot Rodriguez v. Republic of Costa Rica, 139 F. Supp. 2d 173, 188 (D.P.R. 2001) (same); Gutch v. Fed. Republic of Germany, 444 F. Supp. 2d 1, 11 (D.D.C. 2006) (same).
129	It is an open question whether the tort exception requires that both the tortious act or omission *and* the injury or damage must occur in the United States. *Compare* Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 441 (1989) (noting in dicta that the tort exception, unlike the commercial activities exception, does not cover exclusively foreign conduct that has harmful effects in the United States), *with* Restatement (Third) of the Foreign Relations Law of the United States § 454 cmt. e (1987) (construing the tort exception to apply whenever the injury occurs in the United States, "regardless of where the act or omission causing the injury took place."). The plain text of § 1605(a)(5) requires only that the injury or damage occur in the United States. Nevertheless, many lower courts have adopted a territorial restriction on the tortious act or omission, reasoning that, otherwise, foreign states would be overexposed to suit. *See, e.g.,* Persinger v. Islamic Republic of Iran, 729 F.2d 835, 842-43 (D.C. Cir. 1984) (holding that the FSIA tort exception did not apply to the taking of hostages at the U.S. embassy in Tehran, even if it caused emotional distress to families in the United States). This later view finds support in the legislative history. *See* H.R. Rep. No. 94-1487, at 7, 21, *reprinted in* 1976 USCCAN 6605, 6619 (stating that "the tortious act or omission must occur within the jurisdiction of the United States").
130	*Cf.* Cabiri v. Republic of Ghana, 165 F.3d 193, 200 (2d Cir. 1999) ("The FSIA is not an enforcement mechanism for global freedom of information.").

131	First Amended Complaint ¶ 77, Doe v. Ethiopia, No. l:14-cv-00372-CKK (D.D.C. 2014), 2014 WL 916565.
132	*Id.*
133	The Citizen Lab, *Hacking Team's US Nexus,* Research Brief No. 32 (2014), *available at* http://citizenlab.org/2014/02/hacking-teams-us-nexus/.
134	*See, e.g.,* Olsen v. Government of Mexico, 729 F.2d 641, 646 (9th Cir. 1984) (applying tort exception to crash of prisoner transfer flight en route from Mexico to United States), *abrogation on other grounds recognized by* Joseph v. Office of Consulate Gen. of Nigeria, 830 F.2d 1018, 1026 (9th Cir. 1987); Liu v. Republic of China, 892 F.2d 1419 (9th Cir. 1989) (applying tort exception to assassination planned in Republic of China and executed in California); Letelier v. Republic of Chile, 488 F. Supp. 665, 673-74 (D.D.C. 1980) (applying tort exception to assassination planned in Chile and executed in Washington, DC).
135	Asociacion de Reclamantes v. United Mexican States, 735 F.2d 1517, 1525 (D.C. Cir. 1984).
136	*Id.*
137	*Id.*
138	*Olsen,* 729 F.2d at 646.
139	*Id.* at 643-46.
140	*Id.* at 643-47.
141	*Id.*
142	*See* Kozorowski v. Russian Fed'n, 1997 WL 582880, at *4, 124 F.3d 211 (Table) (9th Cir. 1997) (finding one entire tort committed in U.S. territory where Russian news agencies allegedly engaged in a propaganda campaign in the United States that sought to cover up a WWII-era massacre of Polish officers).
143	*Olsen,* 729 F.2d at 646 (emphasis added).
144	Liu v. Republic of China, 892 F.2d 1419 (9th Cir. 1989); Letelier v. Republic of Chile, 488 F. Supp. 665, 673-74 (D.D.C. 1980).
145	*Letelier,* 488 F. Supp. at 673-74 (noting Chilean Republic "set into motion" and prepared a car bombing in Washington D.C. through acts "carried out entirely" within Chile).
146	*Liu,* 892 F.2d at 1419.
147	*Liu,* 892 F.2d at 1433; *Letelier,* 488 F. Supp. at 674.
148	Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 266 (2010) ("[I]t is a rare case of prohibited extraterritorial application that lacks all contact with the territory of the United States.").

149	Foreign sovereign defendants will no doubt urge a stricter reading of the "entire tort" principle, arguing that any foreign conduct in connection to the tort will bar application of the FSIA tort exception. But the only support for this proposition is a line of cases where neither the tortious act, nor the direct injury occurred in U.S. territory. In *Argentine Republic v. Amerada Hess Shipping Corp.,* 488 U.S. 428, 441 (1989), the U.S. Supreme Court held that the bombing of a tanker on the high seas did not trigger the FSIA tort exception, even if financial consequences were eventually felt in the United States. Nothing in *Amerada Hess* would bar applying the FSIA tort exception to the hacking of a computer located in U.S. territory, causing injury to end-users in the United States. Nor would *In re SEDCO, Inc.,* 543 F. Supp. 561, 567 (S.D. Tex. 1982), the case that first coined the "entire tort" formulation. In *SEDCO, none* of the alleged acts or omissions from a Mexican oil rig explosion occurred in the United States--only the consequential injuries. Indeed, none of the cases that adopted *SEDCO's* "entire tort" rule involved a tortious act completed in the United States. *See* Van Dardel v. Union of Soviet Socialist Republics, 736 F. Supp. 1, 7 (D.D.C. 1990) (detention and death of victim in Hungary is not actionable under tort exception); Persinger v. Islamic Republic of Iran, 729 F.2d 835, 842 (D.C. Cir. 1984) (detention of American hostages at U.S. embassy in Tehran not actionable); Jerez v. Republic of Cuba, 777 F. Supp. 2d 6, 25 (D.D.C. 2011) (abuse during psychiatric confinement in Cuba not actionable); Coleman v. Alcolac, Inc., 888 F. Supp. 1388, 1403 (S.D. Tex. 1995) (exposure of U.S. soldiers to chemical weapons in Iraq not actionable); Four Corners Helicopters, Inc. v. Turbomeca S.A., 677 F. Supp. 1096, 1102 (D. Col. 1988) (negligent manufacture of helicopter in France not actionable); Antares Aircraft L.P. v. Fed. Republic of Nigeria, No. 89 CIV. 6513(JSM), 1991 WL 29287 (S.D.N.Y. Mar. 1 1991) (conversion of aircraft in Nigeria not actionable).
150	*See* Joel Brenner, Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World, 54 (2013) (noting that espionage "is no longer a game played only with human spies .... If you can steal terabytes of information electronically, from the comfort of a computer terminal thousands of miles away, perhaps you don't need a spy.").
151	Citizen Lab, Hacking Team, *supra* note 16 (describing spyware attack on Ethiopian language radio station based in Alexandria, Virginia using Remote Control System ("RCS"), a spyware program "sold exclusively to governments by Milan-based [firm] Hacking Team.").
152	*Id.*
153	*Id.; see also* Kim Zetter, *American Gets Targeted by Digital Spy Tool Sold to Foreign Governments,* Wired.com (June 4, 2013 6:30 AM), http:// www.wired.com/threatleveV2013/06/spy-tool-sold-to-governments (discussing suspected surveillance of a U.S. citizen, in the United States, by the Turkish government using RCS spyware).
154	*See, e.g.,* Theofel v. Farey-Jones, 359 F.3d 1066, 1072-73 (9th Cir. 2004) ("Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, ... the [Stored Communications] Act protects users whose electronic communications are in electronic storage with an ISP ...."); Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219, 1230 (N.D. Ill. 2005) (recognizing a trespass to chattels action for the unauthorized installation of spyware on a computer).
155	Katz v. United States, 389 U.S. 347, 352 (1967); *see id.* at 353 ("[I]t becomes clear that the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").
156	Kyllo v. United States, 533 U.S. 27, 34 (2001) ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion ... constitutes a search.") (internal quotations omitted).
157	*See* Am. Online, Inc. v. Nat'l Health Care Disc, Inc., 121 F. Supp. 2d 1255, 1270 (N.D. Iowa 2000) (applying Virginia tort law to the unauthorized access of AOL hardware located in Virginia by spam sent from an Iowa corporation).
158	United States v. Ivanov, 175 F. Supp. 2d 367, 374 (D. Conn. 2001); *see also* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001) (denying suppression of evidence obtained from the Russian computer of a Russian hacker arrested on CFAA charges in the same sting operation as Ivanov); *cf.* Robert Diaz Assocs. Enters., Inc. v. Elete, Inc., No. 03 CIV. 7758 (DFE), 2004 WL 1087468 (S.D.N.Y. May 14, 2004) (holding that "when an unauthorized person 'hacks' into a computer to access, copy or steal files, then personal jurisdiction may be established where the victim's computer is physically located.").
159	*Ivanov,* 175 F. Supp. 2d at 369-70.

160	*Id.* at 371.
161	18 U.S.C. § 2333 (2012).
162	Doe v. Bin Laden, 663 F.3d 64, 65, 70-71 (2011).
163	*Id.* at 67.
164	Liu v. Republic of China, 892 F.2d 1419, 1425 (9th Cir. 1989).
165	28 U.S.C. § 1605(a)(5) (2012) (emphasis added).
166	*See* Willis v. Gordon, 20 Cal. 3d 629, 637 (1978) ("The action for wrongful death is purely a creature of statute, originating in California in an act passed in 1862 (now Code Civ. Proc, § 377) and patterned after Lord Campbell's Act adopted in 1846.").
167	*See* Reiter v. Sonotone Corp., 442 U.S. 330, 339 (1979) (Burger, C.J.).
168	*See* Scalia & Garner, *supra* note 94, at 73.
169	Black's Law Dictionary 1246 (Abridged 8th ed. 2005); *see also* Keeton *et al.,* Prosser and Keeton on the Law of Torts 2 (1984) (defining a "tort" as a "civil wrong, other than breach of contract, for which the court will provide a remedy in the form of an action for damages").
170	Black's, *supra* note 169, at 1246 (defining a "constitutional tort" as a "violation of one's constitutional rights by a government officer, redressable by a civil action").
171	United States v. Burke, 504 U.S. 229, 234 (1992). The *Burke* Court observed that violation of Title VII of the Civil Rights Act is not a tortious personal injury since that title does not provide a remedy. In contrast, in *Curtis v. Loether,* 415 U.S. 189, 195-96 (1974), the Court held that Title VIII "sounds basically in tort" because its fair housing provisions provide for awards of damages. Just like Title VIII, the ECPA and CFAA provide private rights of action and hence sound in tort.
172	*Burke,* 504 U.S. at 235 (quoting Carey v. Piphus, 435 U.S. 247, 257 (1978)).
173	H.R. Rep. No. 94-1487, at 20-21; S. Rep. No. 94-1310, at 20-21S. Rep. No. 94-1310, at 20-21 (emphasis added).
174	*See* H.R. Rep. 94-1487, 13, *reprinted in* 1976 U.S.C.C.A.N. 6604, 6611 (FSIA intended to achieve uniform results in foreign litigation to avoid foreign policy friction); *id.* at 9 (FSIA intended to effect reciprocity with foreign states that deny the United States immunity "in tort and contract cases where the necessary contacts with the forum were present").
175	*See* Cal. Civ. Code § 1708 *et seq.* (codifying torts for battery, domestic violence, and other wrongs).
176	D.C. Code § 16-2701 (negligence causing death).
177	*See* La. Civ. Code Ann. art. 2315 *et seq.* (codifying torts).
178	*Id.* art. 2316.
179	S. Rep. No. 94-1310, at 20S. Rep. No. 94-1310, at 20 (1976).

180	Congress sought to remove unpredictability from immunity determinations. *See* H.R. Rep. 94-1487, 13, *reprinted in* 1976 U.S.C.C.A.N. 6604, 6611 (noting that FSIA was intended to achieve uniform results to avoid foreign policy friction).
181	28 U.S.C. § 1605(a)(5).
182	Alpha Therapeutic Corp. v. Nippon Hoso Kyokai, 199 F.3d 1078, 1088-89 (9th Cir. 1999), *opinion withdrawn on other grounds sub nom*. Alpha Therapeutic Corp. v. Kyokai, 237 F.3d 1007 (9th Cir. 2001).
183	*Id.* at 1089.
184	Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (9th Cir. 2003) (interpreting Stored Communication Act in light of common law trespass); *see also* Neder v. United States, 527 U.S. 1, 23 (1999) (noting "the rule that Congress intends to incorporate the well-settled meaning of the common-law terms it uses.").
185	Black's Law Dictionary 651 (abridged 8th ed. 2005).
186	Bernstein v. Nat'l Broad. Co., 129 F. Supp. 817, 825 (D.D.C. 1955) (quoting Reed v. Real Detective Pub. Co., 63 Ariz. 294, 306 (Sup. Ct. Az. 1945)), *aff'd,* 232 F.2d 369 (D.C. Cir. 1956).
187	Pearce v. E.F. Hutton Grp., Inc., 664 F. Supp. 1490, 1499 (D.D.C. 1987).
188	Reed v. Real Detective Pub. Co., 63 Ariz. 294, 305 (Sup. Ct. Az. 1945).
189	Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193, 205, 213 (1890) (noting that the protection of privacy is one "afforded to thoughts, sentiments, and emotions"); *see also* Dresbach v. Doubleday & Co., Inc., 518 F. Supp. 1285, 1287 (D.D.C. 1981) (noting the injury redressed is one "to the feelings and sensibilities of the person").
190	Berger v. State of N.Y., 388 U.S. 41, 65 (1967) (concurring opinion of Douglas, J.) (emphasis added).
191	28 U.S.C. § 1605(a)(5) (2012).
192	11 U.S.C. § 522(d)(ll)(D) (2012).
193	For example, Section 104(a)(2) of the Internal Revenue Code previously excluded from gross income, damages received "on account of personal injuries or sickness." 26 U.S.C. § 104(a)(2) (1994). Applying common law tort principles, the Supreme Court held that "personal injuries" include a "broad range of physical and nonphysical injuries." United States v. Burke, 504 U.S. 229, 235 n.6(1992).
194	28 U.S.C. § 1605(a)(5)(B) (2012).
195	28 U.S.C. § 1605(a)(5)(A) (2012).
196	28 U.S.C. § 2680(a) (2012).
197	Swarna v. Al-Awadi, 622 F.3d 123, 145 (2d Cir. 2010); MacArthur Area Citizens Ass'n v. Republic of Peru, 809 F.2d 918, 921-22 (D.C. Cir. 1987) (noting that "decisions construing" the FTCA provide "additional guidance on what acts should be deemed discretionary for FSIA purposes"), *amended on other grounds,* 823 F.2d 606 (D.C. Cir. 1987).
198	United States v. Gaubert, 499 U.S. 315, 322-23 (1991).
199	Maalouf v. Swiss Confederation, 208 F. Supp. 2d 31, 35 (D.D.C. 2002).

200	*Gaubert,* 499 U.S. at 322-23 (applying FTCA); *accord* Liu v. Republic of China, 892 F.2d 1419, 1431 (9th Cir. 1989) (applying FSIA).
201	*Gaubert,* 499 U.S. at 323.
202	*See* Working Group of the American Bar Association, *Reforming the Foreign Sovereign Immunities Act,* 40 Colum. J. Transnat'l L. 489, 569-70 (2002) (noting judicial disagreement, but supporting a continued common law approach); Curtis A. Bradley & Jack L. Goldsmith, *Pinochet and International Human Rights Litigation,* 97 Mich. L. Rev. 2129, 2154-55 (1999) (arguing that courts err when considering international law as a constraint on governmental discretion).
203	*See* Letelier v. Republic of Chile, 488 F. Supp. 665, 673 (D.D.C. 1980) (noting that a coordinated assassination obviously involves planning and "policy judgment," yet it nevertheless exceeds the bounds of a foreign state's discretion since it violates national and international law).
204	*See* Berkovitz v. United States, 486 U.S. 531, 544 (1988) ("When a suit charges an agency with failing to act in accord with a specific mandatory directive, the discretionary function exception does not apply."); Hatahley v. United States, 351 U.S. 173, 181 (1956) (holding that acts of wrongful trespass, committed by federal agents in violation of a federal range law, were not discretionary).
205	*Gaubert,* 499 U.S. at 322 (finding no discretion if a "federal statute, regulation or policy specifically prescribes a course of action for an employee to follow"); *Berkovitz,* 486 U.S. at 536 ("the employee has no rightful option but to adhere to the directive.").
206	*See Gaubert,* 499 U.S. at 324 ("If the employee violates the mandatory regulation, there will be no shelter from liability because there is no room for choice and the action will be contrary to policy."); Autery v. United States, 992 F.2d 1523, 1526 (11th Cir. 1993) ("We must first determine whether the challenged act or omission violated a mandatory regulation or policy that allowed no judgment or choice.").
207	*See* Myers & Myers, Inc. v. U.S. Postal Service, 527 F.2d 1252, 1261 (2d Cir. 1975) (observing under the FTCA that "[i]t is ... a tautology that a federal official cannot have discretion to behave unconstitutionally or outside the scope of his delegated authority.").
208	*Gaubert,* 499 U.S. at 323 (quoting United States v. Varig Airlines, 461 U.S. 797, 814 (1984)).
209	Letelier v. Republic of Chile, 488 F. Supp. 665, 673 (D.D.C. 1980).
210	*Id.* ("Whatever policy options may exist for a foreign country, it has no 'discretion' to perpetrate conduct designed to result in the assassination of an individual or individuals, action that is clearly contrary to the precepts of humanity as recognized in both national and international law.").
211	Liu v. Republic of China, 892 F.2d 1419, 1431 (9th Cir. 1989). Previously, the Ninth Circuit had applied *Letelier* in *Gerritsen v. de la Madrid Hurtado,* 819 F.2d 1511, 1516-18 (9th Cir. 1987), finding that Mexican officials had no discretion to assault and kidnap a demonstrator leafleting outside a consulate, as such acts did not "establish governmental policy." *Gerritsen,* however, relied on a now defunct distinction between "planning level" and "operational level" activities rejected by the Ninth Circuit in favor of the *Gaubert* standard. *See id.;* Joseph v. Office of Consulate Gen. of Nigeria, 830 F.2d 1018, 1026 (9th Cir. 1987).
212	MacArthur Area Citizens Ass'n v. Republic of Peru, 809 F.2d 918, 922 n.4 (D.C. Cir. 1987), *modified by* 823 F.2d 606 (D.C. Cir. 1987).
213	*See, e.g., Letelier,* 488 F. Supp. at 673 (holding assassination to be nondiscretionary); *Liu,* 892 F.2d at 1431 (holding assassination to be nondiscretionary).

214	*See, e.g., MacArthur Area Citizens Ass'n,* 809 F.2d at 923 (holding that use of a chancery in violation of D.C. zoning laws was not sufficiently grave so as to render it non-discretionary); Risk v. Halvorsen, 936 F.2d 393, 397 (9th Cir. 1991) (holding that a consular official's issuance of travel documents to a foreign national committing parental kidnapping was too far removed from the crime, and too close to traditional consular duties, to be deemed non-discretionary).
215	*Risk,* 936 F.2d at 397.
216	*Id.* at 394.
217	*Id.* at 397-98.
218	Doe v. Holy See, 557 F.3d 1066, 1083-85 (9th Cir. 2009) (applying *Gaubert* to find that retention and supervision were policy judgments but allowing respondeat superior claims to proceed under tort exception).
219	*See id.* at 1083.
220	*In re* Terrorist Attacks on September 11, 2001, 349 F. Supp. 2d 765, 802 (S.D.N.Y. 2005) *on reconsideration in part,* 392 F. Supp. 2d 539 (S.D.N.Y. 2005) (holding under FSIA that recommending Saudi grants to Islamic charities which allegedly diverted funds to terrorists was a discretionary function) *aff'd on other grounds,* 538 F.3d 71 (2d Cir. 2008) (holding terrorist acts cannot be brought under FSIA tort exception) *abrogated by* Samantar v. Yousuf, 560 U.S. 305 (2010) *and aff'd,* 714 F.3d 118 (2d Cir. 2013) (holding tort exception did not apply because all tortious conduct occurred outside the United States).
221	*MacArthur Area Citizens Ass'n,* 809 F.2d at 924 n.4 (noting that zoning infraction is not a *malum in se* offense such as murder).
222	*See, e.g.,* 18 U.S.C. § 2511(1) (defining crime of wiretapping); *see also* United States v. Szymuszkiewicz, 622 F.3d 701, 703 (7th Cir. 2010) (affirming felony conviction under Wiretap Act for electronic interception of e-mail).
223	*See* Hatahley v. United States, 351 U.S. 173, 181 (1956); Abreu v. United States, 468 F.3d 20, 26 (1st Cir. 2006) ("if the activity in question violates a mandatory federal law ... the exercise of discretion is precluded"); Birnbaum v. United States, 588 F.2d 319, 329-31 (2d Cir. 1978) *abrogated on other grounds, as recognized in* Liranzo v. United States, 690 F.3d 78, 90 n.11 (2d Cir. 2012); Myers & Myers, Inc. v. U. S. Postal Service, 527 F.2d 1252, 1261 (2d Cir. 1975); Orlikow v. United States, 682 F. Supp. 77, 81 (D.D.C. 1988) (noting that in FTCA cases, "[w]hen a decision is made to conduct intelligence operations by methods which are unconstitutional or egregious, it is lacking in statutory or regulatory authority," and outside the discretionary exception to FTCA); Socialist Workers Party v. Att'y Gen. of the United States, 642 F. Supp. 1357, 1417 (S.D.N.Y. 1986) (same); Glickman v. United States, 626 F. Supp. 171, 175 (S.D.N.Y. 1985) (finding in FTCA case that CIA agent's secret administration of LSD to plaintiff was not discretionary function).
224	*Hatahley,* 351 U.S. at 181.
225	*Id.* at 176.
226	*Id.*
227	*Id.* at 180-81.
228	*Id.* at 181.
229	Birnbaum v. United States, 588 F.2d 319, 332 (2d Cir. 1978).

230	*See, e.g.,* Avery v. United States, 434 F. Supp. 937, 944 (D. Conn. 1977) (reasoning that "[i]f trespasses in violation of government regulations are not 'discretionary functions,' [citing *Hatahley]* then, *a fortiori,* trespasses in violation of constitutional guarantees are not 'discretionary functions.'"); Cruikshank v. United States, 431 F. Supp. 1355, 1359 (D. Haw. 1977) (permitting damages action for warrantless surveillance of mail).
231	*Cruikshank,* 431 F. Supp. at 1359.
232	*Id.*
233	Letelier v. Republic of Chile, 488 F. Supp. 665, 673 (D.D.C. 1980) (citing *Hatahley* and *Cruikshank); Liu,* 892 F.2d at 1431 (relying on *Letelier* and holding that foreign officials had no discretion to conduct an assassination in the United States).
234	*See Birnbaum,* 588 F.2d at 329 (holding under FTCA that "a discretionary function can only be one within the scope of authority of an agency or an official, as delegated by statute, regulation, or jurisdictional grant").
235	The Schooner Exchange v. McFaddon, 11 U.S. 116, 136 (1812) (emphasis added).
236	Ian Brownlie, Principles of Public International Law 309 (7th ed., 2008); *see also* S.S. Lotus (France v. Turkey), 1927 Perm. Ct. Int'l. Just. (ser. A) No. 10 (Sept. 7), ¶ 45 ("[T]he first and foremost restriction imposed by international law upon a State is that--failing the existence of a permissive rule to the contrary - it may not exercise its power in any form in the territory of another State."). Note that the consent of an end-user or Internet Service Provider may also be relevant. For example, Article 32b of the Council of Europe's Convention on Cybercrime, to which the United States is a party, states that a: Party may, without the authorization of another Party ... access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the *lawful and voluntary consent of the person who has the lawful authority to disclose the data* to the Party through that computer system. Council of Europe Convention on Cybercrime, Nov. 23, 2001, Art. 32b, T.I.A.S. No. 13,174, E.T.S. No. 185 (emphasis added).
237	*See* Council of Europe, Report of the Cybercrime Convention Committee, Ad-Hoc Sub-Group on Jurisdiction and Transborder Access to Data, Transborder Access and Jurisdiction: What are the Options?, ¶ 37, Dec. 6, 2012 (noting that access to data stored in a foreign jurisdiction is subject to international law limits on territorial sovereignty) [hereinafter, Jurisdiction and Transborder Access].
238	Wolf Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace,* 89 Int'l L. Stud. 123, 126 (2013); *see, e.g.,* The White House, International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World 12-15 (2011) (asserting U.S. jurisdiction over transborder cyber activities); Council of Europe Convention on Cybercrime, Nov. 23, 2001, Arts. 22 (jurisdiction), 31-32 (addressing trans-border investigations), T.I.A.S. No. 13,174, E. T.S. No. 185.
239	International Strategy for Cyberspace, *supra* note 238, at 12-14.
240	*See In re* 840 140th Ave., 634 F.3d 557, 562-64 (9th Cir. 2011) (discussing framework for letters rogatory and mutual legal assistance treaties).
241	*See* U.S. Dept. of State Foreign Affairs, 7 FAM 960, Criminal Matters, Requests from Foreign Tribunals, and Other Special Issues (2013), *available at* http://www.state.gov/documents/organization/86744.pdf.
242	*See* Jurisdiction and Transborder Access, *supra* note 237, ¶ 37; U.N. Office on Drugs and Crime, Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime, at 9, U.N. Sales No. E.09.XI. 19 (2009) (noting that "[t]he use of electronic evidence gathering in another jurisdiction will require a request from the investigating jurisdiction to the country in which surveillance is anticipated to occur.").
243	*See In re* 840 140th Ave., 634 F.3d at 572 ("We therefore hold that, in the context of an MLAT request, a district court may not enforce a subpoena that would offend a constitutional guarantee.").

244	United States v. Gaubert, 499 U.S. 315, 324 (1991).
245	18 U.S.C. § 951(a) (emphasis added). Section 951(d) defines the term "agent of a foreign government" as an "individual who agrees to operate within the United States subject to the direction or control of a foreign government or official" but excluding accredited diplomats or consular officials or "any officially and publicly acknowledged and sponsored official or representative of a foreign government." The Attorney General has promulgated notification regulations through the Foreign Agent Registration Act. 28 C.F.R. Part 5.
246	United States v. Soueid, Statement of Facts, No. 1:11-cr-494 (E.D.Va. Mar. 26, 2012); *judgment entered pursuant to plea agreement,* No. 1:11-cr-00494 (E.D. Va. Jul. 24, 2012).
247	United States v. Dumeisi, 424 F.3d 566, 569-70 (7th Cir. 2005) (affirming judgment).
248	Granted, cyber intruders do not personally enter the United States. They do not need to: the Internet permits them to carry out remote operations. Courts have yet to address whether remotely deploying malware in a computer located in the United States and intercepting U.S. communications is "act[ing] in the United States" for purposes of § 951. Nonetheless, the analogy stands: if state agents lack discretion to eavesdrop in the United States by analog means, they should not have discretion to eavesdrop by digital means.
249	*Cf.* Hatahley v. United States, 351 U.S. 173, 180 (1956); Birnbaum v. United States, 588 F.2d 319, 329 (2d Cir. 1978).
250	In brief, these activities include the bulk collection of phone metadata inside the United States; the collection of the contents of communications of non-U.S. persons from U.S.-based companies under the PRISM program; and the tapping of fiber-optic cables in U.S. territory that carry global internet traffic, under the UPSTREAM program. This Article takes no position on the legality or propriety of these activities. For background on the U.S. government's internet surveillance programs, *see* President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World 132--41 (Dec. 12, 2013), available at http:// www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; *The NSA Files,* The Guardian, http://www.theguardian.com/world/the-nsa-files (last visited Feb. 8, 2015).
251	*See, e.g.,* Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 10-11 (Jan. 23, 2014), *available at* http://www.pclob.gov/meetings-and-events/2014meetingsevents/23-january-2014-public-meeting (concluding bulk phone metadata collection violates the ECPA); Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism,* Fordham L. Rev. (forthcoming) at 13 (Jan. 23, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2383976 (arguing that counterterrorism surveillance complies with international human rights law).
252	U.N. Human Rights Comm., Concluding observations on the fourth report of the United States of America, Advance Unedited Version, ¶ 22, adopted at 110th Sess. (Mar. 10-28, 2014) (urging the United States to comply with international privacy rights in its surveillance of domestic and foreign targets).
253	Indeed, Germany has already announced the opening of a judicial investigation into the United States' interception of phone calls made by Chancellor Angela Merkel and the monitoring of German citizens' communications in Germany. Christian Rath, *"Wir sind nicht die NSA",* Die Tageszeitung (Mar. 17, 2014), http://www.taz.de/!134944/; *see also* Ryan Gallagher, *Der Spiegel: NSA Put Merkel on List of 122 Targeted Leaders,* The//Intercept (Mar. 29, 2014, 10:07 AM), https://firstlook.org/theintercept/article/2014/03/29/der-spiegel-nsa-ghcq-hacked-german-companies-put-merkel-list-122-targeted-leaders/.
254	For a discussion of the role of prudence and justiciability in judicial decision-making, *see generally* Alexander M. Bickel, The Least Dangerous Branch: The Supreme Court At The Bar Of Politics 183-97 (1962).
255	*See* Mark Tushnet, *Law and Prudence in the Law of Justiciability: The Transformation and Disappearance of the Political Question Doctrine,* 80 N.C. L. Rev. 1203, 1203-22 (2002) (discussing the doctrinalization of prudential concerns through the political question and standing doctrines).
256	Bickel, *supra* note 254, at 125.

257	*See, e.g.,* El-Shifa Pharm. Indus. Co. v. United States, 607 F.3d 836 (D.C. Cir. 2010) (en banc) (holding that political question doctrine barred judicial review of U.S. cruise missile attack on Sudanese pharmaceutical factory accused of producing material for chemical weapons); Corrie v. Caterpillar, Inc., 503 F.3d 974 (9th Cir. 2007) (holding that political question barred consideration of an Alien Tort Statute action brought by family members of a U.S. citizen killed when Israeli Defense Forces used bulldozers manufactured and sold by a U.S. company, allegedly with knowledge they would be used to violate international law); Bancoult v. McNamara, 445 F.3d 427 (D.C. Cir. 2006) (holding that political question doctrine barred damages action brought by Chagos islanders against U.S. government for forced removal); *see generally* Stephen I. Vladeck, *The New National Security Canon,* 61 Am. U. L. Rev. 1295, 1321 (2012) (noting courts' increasing reliance on the political question doctrine since September 11, 2001).
258	*See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013) (holding that civil liberties organizations lack standing to challenge statute authorizing interception of communications with non-U.S. persons because they could not show evidence that their communications with foreign clients or contacts had been monitored); Du Daobin v. Cisco Sys., Inc., CIV. PJM 11-1538, 2014 WL 769095, at *6-7 (D. Md. Feb. 24, 2014) (applying political question and act of state doctrines to dismiss claims alleging that Cisco aided and abetted torture in China by supplying China with internet monitoring equipment).
259	The territorial tort exception to foreign state immunity is a feature of the "restrictive doctrine" of immunity that was broadly accepted by the international community in the course of the 20th Century. *See generally* Hazel Fox, The Law of State Immunity, 309-21 (2002) (stating that "independently of UNSCI the overwhelming majority of States supports a restrictive doctrine"); Rosanne Van Alebeek, The Immunity of Foreign States and Their Officials in International Criminal Law and International Human Rights Law, 16--17, 67-70 (2008) (stating that "keeping in mind the natural limits of a state's *imperium* it is more appropriate to say that the territorial tort exception as included in almost all national codifications of the state immunity rule ... is the reflection of the jure *imperri-jure gestionis* distinction"). Like the FSIA, other states' immunity laws make an exception for personal injuries or property damage occurring in the territory of the forum state. *See, e.g.,* U.K. State Immunity Act, § 5, 1978, reproduced in 17 I.L.M. 1388 (1978) (providing exceptions for "death or personal injury" or "damage to or loss of tangible property, caused by an act or omission in the United Kingdom."). The United States has itself been a defendant in such lawsuits overseas. In the *Holubek* case, for example, the Austrian government rejected the United States' plea of foreign sovereign immunity in a case involving a motor accident caused by the negligent driving of a U.S. government-owned car. The Austrian Supreme Court ruled that "[b]y operating a motor car and using public roads the defendant moves into spheres in which private individuals also move. In these spheres the parties face one another on a basis of equality, and there is no indication here of any supremacy and subordination." Collision with Foreign-Government-Owned Motor Car (Austria) Case, 40 I.L.R. 73 (Aus., S. Ct. 1961). Another example is the case of *United States v. Reyes,* G.R. No. 79253 (Mar. 1, 1993 Sup. Ct. Philippines), *available at* http:// www.lawphil.net/judjuris/juri1993/mar1993/gr_79253_1993.html, where the Supreme Court of the Philippines denied the United States' plea of immunity in a discrimination lawsuit brought by a U.S. employee stationed on a Joint U.S. Military Assistance Group base.
260	Alfred Dunhill of London, Inc. v. Republic of Cuba, 425 U.S. 682, 691 n.7 (1976) (quoting Underhill v. Hernandez, 168 U.S. 250, 252 (1897)); Banco Nacional de Cuba v. Sabbatino, 376 U.S. 398, 428 (1964).
261	Liu v. Republic of China, 892 F.2d 1419, 1433 (9th Cir. 1989).
262	*See* Republic of Iraq v. First Nat. City Bank, 353 F.2d 47, 51-52 (2d Cir. 1965) (holding that when property confiscated by a foreign state is located within the United States at the time of attempted confiscation, the foreign act of state can be given effect only if it is consistent with policy and law of United States).
263	*Liu,* 892 F.2d at 1432-33 (holding that act of state doctrine did not preclude liability for assassination committed in California); Letelier v. Republic of Chile, 488 F. Supp. 665, 673-74 (D.D.C. 1980) (rejecting act of state defense).
264	*Letelier,* 488 F. Supp. at 674.
265	Baker v. Carr, 369 U.S. 186, 211 (1962).

266	In 1962, the *Baker* Court's famous criteria for political questions included six factors. *Id.* More recently, however, the Supreme Court seems to have narrowed the field to two. *See* Zivotofsky *ex rel.* Zivotofsky v. Clinton, 132 S. Ct. 1421, 1427 (2012) (noting only two circumstances under which a case presents a political question); Nixon v. United States, 506 U.S. 224, 228 (1993) (same); *see also* Chris Michel, Comment, *There's No Such Thing as a Political Question of Statutory Interpretation: The Implications of* Zivotofsky v. Clinton, 123 Yale. L.J. 253, 260 (2013) (arguing that *Zivotofsky* effectively precludes applying the political question doctrine to bar review of statutory claims).
267	*Baker,* 369 U.S. at 217.
268	*Id.*
269	El-Shifa Pharm. Indus. Co. v. United States, 607 F.3d 836, 856 (D.C. Cir. 2010) (Kavanaugh, J., concurring) ("The Supreme Court has never applied the political question doctrine in a case involving alleged *statutory* violations. Never.").
270	Michel, *supra* note 266, at 259-62.
271	*Zivotofsky,* 132 S. Ct. at 1428.
272	*Id.*
273	*See id.* at 1428 ("[T]here is, of course, no exclusive commitment to the Executive of the power to determine the constitutionality of a statute.").
274	*Id.*
275	*See, e.g.,* Kaplan v. Cent. Bank of Islamic Republic of Iran, 961 F. Supp. 2d 185, 193 (D.D.C. 2013) (concluding under *Zivotofsky* that whether attacks in Israel were acts of war or terrorism, as defined in the Anti-Terrorism Act, is not a political question).
276	Samantar v. Yousuf, 560 U.S. 305, 313 (2010) (FSIA aimed to "transfer primary responsibility for deciding claims of foreign states to immunity from the State Department to the courts") (internal quotations omitted).
277	*See, e.g., id.* at 314--15 (construing "agency and instrumentality" so as not to include individual officials).
278	United States v. Gaubert, 499 U.S. 315, 323 (1991).
279	*See* Stanford v. Texas, 379 U.S. 476, 483-84 (1965) (discussing *Entick* and considering its opinion "a wellspring of the rights now protected by the fourth amendment"); Thomas, *Stumbling Toward History, supra* note 6, at 210-11.
280	*See* 2 Matthew Hale, The History of the Pleas of the Crown 151 n.5, ch. XVIII, II.3. (1736) (by implication).
281	Entick v. Carrington, 19 Howell's State Trials 1029, 1030-32, 95 Eng. Rep. 807 (C.P. 1765).
282	*Id.*
283	*Id.* at 1074.
284	Eric Schnapper, *Unreasonable Searches and Seizures of Papers,* 71 Va. L. Rev. 869, 875-76 (1985); Thomas, *Stumbling Toward History, supra* note 6, at 210-12.

285	Leach v. Money, 19 Howell's State Trials 1002, 97 Eng. Rep. 1050, 1075 (KB. 1765); Wilkes v. Halifax, 19 Howell's State Trials 1406 (C.P. 1769); Entick v. Carrington, 19 Howell's State Trials 1029, 95 Eng. Rep. 807 (C.P. 1765); Wilkes v. Wood, Lofft 1, 19 Howell's State Trials 1154, 98 Eng. Rep. 489 (C.P. 1763); Beardmore v. Carrington, 19 Howell's State Trials 1405 (C.P. 1763); Huckle v. Money, 19 Howell's State Trials 1404, 95 Eng. Rep. 768 (C.P. 1763).
286	Thomas, *Stumbling Toward History, supra* note 6, at 213.
287	Arthur H. Cash, John Wilkes: The Scandalous Father of Civil Liberty 105 (2006).
288	*See, e.g.,* United States v. Jones, 132 S. Ct. 945, 949-50 (2012) (discussing *Entick* and the influence of common-law trespass on Fourth Amendment jurisprudence addressing new technologies).
289	*See supra,* notes 223-32 and accompanying text.
290	*Immunities of Foreign States: Hearings on H.R. 3493 Before the Subcomm. on Claims and Governmental Relations of the House Comm. on the Judiciary,* 93d Cong., 29 (1973) (testimony of Bruno Ristau, Chief, Foreign Litigation Section, Civil Division, U.S. Department of Justice) (emphasis added).
291	*See generally* Fox, *supra* note 259 (surveying personal injuries exception to immunity in the practice of common law and civil law states).
292	Inmunidad Jurisdictional de los Estados Extranjeros Ante los Tribunales Argentinos [Act on the Immunity of Foreign States from the Jurisdiction of Argentine Courts], Ley N° 24.488, art. 2° d), published in the *Boletín Oftcial* of June 28, 1995 [Arg.].
293	Foreign State Immunities Act, Act No. 196 of 1985, § 13 [Austrl.].
294	State Immunity Act, RSC 1985, c S-18, § 6 [Canada], *available at* http://canlii.ca/t/lgjj.
295	Foreign States Immunity Law, Law 5769-2008, § 5, Nov. 5, 2008 [Isr.].
296	Act on the Civil Jurisdiction of Japan with respect to a Foreign State, Act. No 24 of Apr. 24, 2009, art. 10 [Japan], English translation *available at* http://www.japaneselawtranslation.go.jp/law/detail/? id=1948&vm=04&re=02.
297	State Immunity Act, Act 19 of 1979, § 7, Oct. 26, 1979, revised 1985 [Sing.].
298	Foreign States Immunities Act 1981, § 6. [S. Afr.].
299	State Immunity Act 1978, § 5, 17 I.L.M. 1123 (1978) [U.K.].
300	Christian Rath, *"Wir sind nicht die NSA",* Die Tageszeitung (Mar. 17, 2014), http://www.taz.de/!134944/, *discussed in* Ryan Gallagher, *Der Spiegel: NSA Put Merkel on List of 122 Targeted Leaders,* The//Intercept, (Mar. 29, 2014), https://firstlook.org/theintercept/article/2014/03/29/der-spiegel-nsa-ghcq-hacked-german-companies-put-merkel-list-122-targeted-leaders/.
301	International Strategy for Cyberspace, *supra* note 238, at 12 ("The United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies."); *id.* at 14 ("We reserve the right to use all necessary means--diplomatic, informational, military, and economic--as appropriate and consistent with applicable international law ....").
302	Scott Neuman, *Obama Authorizes New Sanctions On North Korea Over Sony Hack,* Nat'l Public Radio, (Jan. 2, 2015), http://www.npr.org/blogs/thetwo-way/2015/01/02/374598365/obama-authorizes-sanctions-on-n-koreaover-sony-hack.

303	*See* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About,* 37 Yale J. Int'l L. Online 11, 12-18 (2011); Blumenthal, *supra* note 23.
304	Jeremy A. Rabkin and Ariel Rabkin, *Why the Current Law of Armed Conflict Should Not Fetter U.S. Cyber Strategy, in* Emerging Threats in National Security and Law 10 (ed. Peter Berkowitz, 2012), http:// media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf.
305	United States v. Dong, Indictment, No. 14-118 (W.D. Pa. May 19, 2014), available at http:// www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf.
306	*See* Charles Doyle, Congressional Research Service, Corporate Criminal Liability: An Overview of Federal Law 3 (2013) (noting "judicial reluctance, absent explicit language, to conclude that Congress intends to expose governmental entities to punitive measures"); *cf.* Stuart P. Green, *Municipal Criminal Liability,* 72 N.C. L. Rev. 1214-21 (1993-94) (discussing extreme rarity of prosecuting local governments under federal criminal law).
307	Conner v. Tate, 130 F. Supp. 2d 1370, 1374 (N.D. Ga. 2001) (holding that although "a governmental entity ... could not be prosecuted criminally for a violation of the Wiretap Act," it could be held civilly liable).
308	*See supra* notes 108--10 and accompanying text.
309	28 U.S.C. § 1606 (stating that a foreign state shall be liable as to any claim for which it is not entitled to immunity).
310	*Id.* ("[A] foreign state except for an agency or instrumentality thereof shall not be liable for punitive damages.").
311	18 U.S.C. § 2520 (authorizing courts to assess damages at the greater of $100 a day for each day of violation or $10,000).
312	*See* Fouad Ajami, *The Arab Spring at One: A Year of Living Dangerously,* Foreign Affairs, Vol. 91, No. 2 (2012): 56-65 (describing waves of protest and calls for democracy and civil liberties across Middle East and North Africa); Reporters Without Borders, *Enemies of the Internet Report,* 4 (2012), *available at* http://en.rsf.org/beset-by-online-surveillance-and-12-03-2012,42061.html (tying internet surveillance and censorship to emergence of online networks of dissident bloggers and activists in Arab Spring).
313	Robert H. Jackson, June 7, 1945 Report to the President on Atrocities and War Crimes, U.S. Dept. of State Bulletin § III (1945).