Cyber-Terrorism and the Private Sector: Responses and Liabilities

Moderator: Professor Karen J. Greenberg, Fordham Law School

Panelists: David F. Snively, Secretary and General Counsel, Monsanto Company
Richard Salgado, Director of Law Enforcement, Google
Honorable Louis J. Freeh, Freeh Group International Solutions, LLC
John Thorne, Kellog Huber Hansen Todd Evans & Figel PLLC

The Judicial Conference concluded with a panel that explored cyber-crime and cyber-terrorism from the perspective of the private sector. A panel featuring voices from academia, prior government service, and corporate leadership, provided an important complement to earlier panels that had explored governmental responses to, and perspectives on, the cyber-threat.

Professor Karen J. Greenberg, Director of the Center on National Security at Fordham Law School, moderated the panel. Professor Greenberg began the panel discussion by stating that the purpose of the panel was to discuss the "elephant in the room" from the prior days' discussions: the role of the private sector in protecting our security and, more importantly, "what should be the role of the private sector in its relationship to government." Professor Greenberg indicated that she intended the panel to address the "conversation" between the government and the private sector concerning civil liberties, regulation and the rights of corporations to make their profits. She asked John Thorne, former Deputy General Counsel of Verizon Communications, to commence the discussion by expressing his views concerning the responsibilities, liabilities and future of private sector regulation in the cyber-age.

Mr. Thorne commenced by relating how, when he was still working at Verizon, he was first asked to address cyber-security and privacy issues in the mid-2000s after Verizon acquired assets of telecommunications provider MCI and the company had to upgrade its infrastructure to integrate those assets. Mr. Thorne stated that Verizon determined that substantial investments in

security and privacy would benefit the company by helping it to enable a "more secure, more private, better experience for customers," and help it increase market share. He stated that their efforts resulted in increased consumer confidence in the company, but that the process was an intensive one, somewhat like "undergoing an audit" to determine the company's weaknesses and vulnerabilities. Mr. Thorne recommended that judges evaluating evidentiary issues involving cyber-matters consider creating what he described as an "audit privilege" to encourage companies to inspect themselves, identify opportunities for improvement and track reforms that they make without risking adverse legal consequences as a result of their awareness of vulnerabilities.

Mr. Thorne then turned to the current state of the law concerning communications firms, other private enterprises and critical infrastructure. He stated that the "good news for critical infrastructure companies is that almost everything at the moment is completely voluntary" due to the absence of statutes or binding codes of conduct governing how critical infrastructure firms need to act in the cyber-world. The "bad news," however, was that the absence of regulation creates a "terrific opportunity for exposure when something goes wrong and the very flexible tort and contract doctrines are available for people who want to create a case if something bad happens to their information or something terrible happens that knocks out the things that rely on the critical infrastructure." Mr. Thorne recommended adoption of a standard process developed by the National Institutes of Standards and Technology called the "Framework for Improving Critical Infrastructure Cybersecurity" (the "NIST Framework") to help figure out vulnerabilities and to address and track the necessary improvements.[4] Mr. Thorne stated that a significant motivation in today's world for adequately protecting information is that if the information is not protected properly, "you're going to lose your job." He noted a further motivation: inadequate data protection could result in adverse action by the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC"), among other federal regulators, citing examples of recent actions and statements by those regulators in which, among other things, a company's inadequate control of customer data could constitute an "unfair and deceptive" act subject to sanction by the FTC. He noted, however, that the NIST Framework has to be adopted by top management of a company to be successful and to guard against potential liability.

Professor Greenberg then asked Richard Salgado, a former federal prosecutor and now a Google executive, how the revelations by Edward Snowden concerning the government's covert efforts in the cyber-world affected the conversation between government and the private sector concerning cyber-matters. Mr. Salgado started by stating that, at Google "privacy and security are really kind of the same thing." Google is interested in protecting the data of all users, no matter where in the world they are located, from "those who have no authorized access to their data." Those without authorized access might include hackers from foreign nation-states or actors within the United States, including intelligence services. Mr. Salgado related that Google first experienced the issue in a significant way in 2009 when Chinese hackers intruded into the Google network. He stated that Google decided, "we were

[4] A copy of the NIST Framework is available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

not going to be shamed by it, we were going to investigate like crazy" to "figure out what happened, fix our systems, get secure so it doesn't happen again and catch it if there are any attempts." The information gained from the investigation then was reported to the government and to other companies that Google determined may have suffered from the same attack. After Google went public with the attack and its response to it, other companies started disclosing their own experiences with cyber-attacks, leading Mr. Salgado to conclude that Google's efforts may have broken "some sort of shame barrier" that had been keeping other companies from talking about cyber-security issues that they were experiencing from China and other jurisdictions. Over time, as Mr. Salgado reported, the culture of companies had changed to "working with each other to share vulnerability information and help each other out in the investigations."

Mr. Salgado related that, while information-sharing among companies has proven successful, it has "proven tricky once you introduce government into that." This concern arises because the law imposes restrictions on the types of information that can be shared with the government. There are risks that the government will take "aggressive action against the company" and result in businesses turning over more data to the government if issues are brought to the government's attention. In Mr. Salgado's view, the role of government in these conversations among companies was not fully worked out, and there are "a lot of improvements that need to be made."

Responding to Professor Greenberg's question, Mr. Salgado stated that the revelations concerning Edward Snowden had not affected Google's approach to security significantly because Google's approach to security was and continues to be "all about keeping data secure from those that aren't authorized to see it," including state actors. He indicated that stories relating to federal intelligence services' alleged secret efforts to weaken security in products to make it easier to breach encryption and to pick up communications between data centers were "of concern" and that Google's reaction was to "find where those vulnerabilities are and to secure them so there aren't ways to get the data that aren't part of the legal regime" through the criminal or national security legal processes. He stated that the Snowden revelations prompted Google to speed up encryption and other security efforts that already were underway before the revelations. Mr. Salgado also reported that the revelations have caused Google to review legal authorities in the United States and to work hard, "not only to be transparent with users about the demands" from government under the current legal regime, but to try to "update the laws to make them match what users should usually expect will happen to their data when the government comes knocking on Google's door."

Professor Greenberg then asked former FBI Director and United States District Judge Louis J. Freeh to offer his perspective on the role the government should play in cyber-security. Judge Freeh began by relating that issues concerning technology, security and privacy had been faced by the country since the days of Benjamin Franklin, who used to write and struggle with the balance between liberty and security. He stated that if those issues were hard in the 18th century, they are "exquisitely complex" now, too exceptional of a problem for the government to address by itself. He gave as an example the creation of the Economic Espionage Act in the 1990s, which enabled the government to prosecute cyber-thefts of intellectual property. He related that the State Department raised objections to the Act because it was concerned that

the word "espionage" would be offensive to most of those who were stealing our intellectual property, who were "our closest allies." Judge Freeh related that the sophisticated and problematic political issues related to intellectual property made it difficult for the government to organize and deal with economic espionage. He indicated that, as a result, the government can play a role in protecting intellectual property, but it "can't play a controlling role" in that effort. He cited as a further example the fact that in the 24 months it takes to develop and adopt a government regulation, computing power doubles, and that technological change often outpaces the ability of government to regulate it.

Professor Greenberg then turned to David F. Snively, and asked him for practical examples, based on his experiences at Monsanto, of how a company guards against and responds to cyber-attacks. Mr. Snively explained that cyber-security now sits "at the top of any board of directors' list of concerns." He explained that, for Monsanto, a science company that focuses on agriculture, intellectual property is its "crown jewels." He stated that to protect those "crown jewels," the company has developed substantial resources for monitoring its Information Technology ("IT") and security systems around the globe. It has mapped all of its information to determine where it is housed, so that if there is a loss or a breach, "we can at least understand where our vulnerabilities are." He revealed that, despite this effort, Monsanto is "attacked on average 490,000 times a month." Due to the sheer volume of attacks, and the presence of subsidiaries and employees around the world who have personal devices or computers, there have been occasions in which attacks have breached Monsanto's security.

Mr. Snively gave as an example a recent occasion on which state-sponsored hackers attempted to access Monsanto's headquarters and its Silicon Valley presence, but they did not succeed. Those same hackers, however, were able to breach the cyber-security systems of a recently-acquired subsidiary and access the subsidiary's data systems for a brief period of time before the breach was detected. He described the intrusion as being contained quickly and addressed in a relatively straightforward manner. However, because the intrusion had accessed the "top levels of the servers in that subsidiary," and it was not possible to determine whether the intruders had accessed data hosted on that subsidiary's servers, including private information concerning employees and customers of the subsidiary, it became necessary under state privacy laws to carry out procedures to notify those employees and customers of the breach, which then prompted media reports on the breach and potential adverse business consequences as the breach was publicized. The company also determined that it would cover costs of all of the employees' and customers' issues arising out of the breach, including credit searches. Disclosures to state attorneys general and governments located abroad were necessary. He described the undertaking as an expensive one, even where, as in that case, the breach was detected quickly and it was impossible to determine if anything of value was taken. Mr. Snively stated that the high costs were not uncommon — that data breaches, on average, cost Monsanto $3 million per breach to address.

Mr. Snively explained further that Monsanto has developed a threat matrix concerning the cyber-threat with three bundles: advanced, persistent threats, which include state-sponsored attacks and sophisticated hackers like LulzSec and Anonymous; generalized activist groups who engage in cyber-attacks; and internal threats in which an employee, accidentally

or on purpose, breaches the company's cyber-security. He described the internal threat as the most serious one because internal actors are "the people you trust," who are "going to get all the way to the edge of your crown jewel data" and cause substantial issues if the data is lost or stolen.

Professor Greenberg then asked Mr. Snively whether information on data breaches and responses was shared within his industry, and whether this cut against the argument that the private sector cannot respond effectively to the cyber-threat because of its interests in avoiding public disclosures that risk reputational harm. Mr. Snively replied that, generally, information was not shared within the industry for competitive reasons, but that Monsanto did share information about cyber-threats with other companies in the IT industry, and it had a policy of communicating breaches of cyber-security properly. He described the company's approach to the cyber-threat "almost as a standing crisis management approach," in which the company was prepared to respond quickly and effectively to cyber-threats and access resources either inside or outside its sector.

Judge Freeh added that disclosure issues were complicated by corporate fiduciary duties and regulatory issues. He explained that, with respect to publicly traded companies, material breaches of cyber-security might have to be reported to an auditor, which could then lead to a debate concerning whether a breach was material enough to warrant a public disclosure. A decision to disclose then could prompt law enforcement agents to ask that the information not be disclosed publicly because of an ongoing investigation, which would raise very difficult issues for companies as they attempted to balance competing interests. Judge Freeh added that, "as these breaches get more material and more serious and the calculation of a loss much more difficult, you have to make a call and it's a very, very significant mistake to make if you make one."

Mr. Snively responded to Judge Freeh's comment by stating that Monsanto's response to cyber-breaches, as decided by the company's board of directors, was to disclose if there is any material breach, even if it adversely affects a government investigation, because of the risks to the company of non-disclosure.

Professor Greenberg then asked the panelists whether they foresaw legislation that would mandate particular approaches to the cyber-threat, and how companies would react if that happened. Mr. Thorne replied that, while there were many proposals for legislation, it would be hard to craft legislation that would be adopted. Mr. Thorne responded to comments earlier in the Conference by former U.S. Senator Joseph Lieberman in which he stated that in the absence of legislation, there would be massive exposure for private companies, by stating that he believed courts and regulatory agencies addressing breaches of cyber-security had the ability to fashion rules that limited companies' liability in an appropriate way.

Professor Greenberg then asked Mr. Salgado to address whether a conflict had developed between the IT industry and the government over the proper approach to the cyber-threat. She alluded to recent assertions by Microsoft that it would not cooperate with the government in providing certain information going forward and earlier similar statements by Yahoo! that appeared to reflect that "there has been a defiant sense on the part of industry."

Professor Greenberg asked why the conflict had developed, and what the IT industry was trying to protect through the conflict: "Is it your profits? Is it your sense of self, your identity?"

Mr. Salgado replied that he did not think that there was a war going on between the IT industry and government. He explained that Google and other Silicon Valley companies have a "very libertarian culture" in which there was a "great deal of suspicion around government intrusion into the privacy of the users' data." He also observed that the laws concerning privacy had not been keeping up with "what's really happening in the world," which was that information that used to be stored in homes is now getting out to the Internet, where it is stored and relied upon by users. He explained that the governing statute, the Electronic Communications Privacy Act, dated from 1986, is "a long time in Internet time." In Mr. Salgado's view, the third-party doctrine of *Smith v. Maryland*, under which information held by third parties is not entitled to Fourth Amendment protections, is not compatible with today's world, because "to live in today's modern world and participate in the modern economy you're going to have a hard time staying away from" companies that hold private information. Mr. Salgado indicated that he saw momentum towards changing the laws to increase privacy, but that this was not a war as much as a desire in the IT industry to change the rules to increase privacy protections for users. He indicated that this conflict over existing law is, in some cases, playing out in the courts as companies begin challenging government data-collection efforts and programs, such as novel requests under the Foreign Intelligence Surveillance Act or requests for bulk data collection under the Patriot Act.

Professor Greenberg then asked Judge Freeh how he saw the role of government, the courts and private companies developing over time. Judge Freeh replied that he did not believe "volunteerism" by companies to address cyber-threats would be sufficient, given that voters and consumers do not believe that private companies are meeting their expectations concerning cyber-security. He cited as an example the SEC's recent move to require financial institutions to disclose cyber-security plans, vulnerability assessments and other matters in response to SEC inspections and examinations. Judge Freeh also observed that courts in the First and Fourth Circuits are considering whether to impose tort liability on service providers if there are data breaches so that losses do not fall only on consumers. The disconnect between corporations' efforts, while diligent, and expectations and political demands, has led Judge Freeh to conclude that legislation in the field is inevitable.

Professor Greenberg then asked the panelists to discuss whether the growing cyber-threat is coming more from corporate criminals versus state actors. Mr. Thorne replied that he lacked statistics on the sources of the threats, but he noted that what is known as the "Internet of things" — the connection to the Internet of more and more devices — was growing exponentially, so that by 2020 "we will have added 50 billion more things to the Internet." Mr. Thorne indicated that increased connectivity would result in more vectors for different actors to attack, making it critical for both government and private actors to do more to guard against threats.

Mr. Salgado replied that, while he could not divide up the source of attacks between private and state actors, Google is under "constant attack." He gave as an example Distributed

Denial of Service ("DDOS") attacks, which he asserted were constantly being attempted against Google, sometimes in significant ways. Mr. Salgado replied that Google had developed a high ability to absorb and fend off DDOS attacks, but it was not possible to know the motive for the attacks — whether attackers are just "angry at somebody's blog post or trying to make some bigger point."

Mr. Salgado added that, following the 2009 attack from China, Google developed a robust network security program that enables Google to determine whether phishing emails are being sent from particular actors to particular types of users, such as state actors who may target government employees' Gmail accounts for intrusion. He stated that when these attacks are detected, Google not only blocks the emails, it also informs users that it believes they have been targeted by state-sponsored attackers and advises them to take steps to secure their accounts.

Professor Greenberg asked Mr. Salgado whether Google informs the government when it detects such attacks. He replied that while the user can inform the government, Google does not. Mr. Salgado stated that, while Google has teams that investigate crimes and reports them to the government, it is very cautious about turning over user information to the government, particularly where the user is a victim. Its policy is to let users decide whether they want to be involved in a criminal investigation. It is only where a "bad guy" is detected that a referral may be made, and even in that case, legal process is necessary for there to be further disclosures so that it is all "very tight and user privacy oriented."

Judge Freeh added that there were two types of significant threats to cyber-security: internal threats and external threats. He described the internal threat as "huge, unmeasured and really uncontrolled." With respect to external threats, Judge Freeh described the state actors as "clearly the heavy lifters" in the arena. He explained that some state actors had "the potential and the wherewithal to literally shut down other countries and their systems and their infrastructure." He explained that it is not done, just as our nation does not shut down banking channels used by terrorists, even though we could, because of the negative repercussions that would flow from shutting down third-party banking systems. He analogized it to experience during cold war where "everyone had these massively destructive weapons, [but] no one actually used them." He added that some state actors even in radical regimes had the ability to inflict significant damage but did not do so due to practical, economic and personal constraints. The increased capabilities of non-state actors, however, changed the dynamic because they "don't have the hesitations and controls that a state actor might have."

Professor Greenberg asked Mr. Snively whether he had "better news than that." He replied that he did not. He explained that the cyber-threat was real and not going to stop and that Monsanto constantly was under threat by state actors and others who would attempt to steal its intellectual property. He added that judges also needed to pay attention to the cyber-threat in order to ensure the integrity of the legal system "because there's a lot of money that's going to change hands in this arena and this is something you're going to live with every day."

Professor Greenberg concluded the panel by citing the need for public education "so that the kinds of threats that need to be taken seriously can be taken seriously and can be addressed as an issue."