

## privacy and cybersecurity lawflash

December 10, 2014

## DOJ Announces New Cybersecurity Unit in the Criminal Division

*To address cyber threats on multiple fronts, the DOJ is creating a new Cybersecurity Unit with the goal of having both a robust enforcement strategy as well as a broad prevention strategy.*

In a significant advancement toward combating cyber threats, last week, Assistant Attorney General Leslie R. Caldwell, the head of the Criminal Division for the U.S. Department of Justice (DOJ), announced the creation of a new Cybersecurity Unit.<sup>1</sup> She recognized the need to “address cyber threats on multiple fronts, with both a robust enforcement strategy as well as a broad prevention strategy.”

### “Central Hub” on Cybersecurity Issues and Guidance

As Ms. Caldwell outlined, the prosecutors in the new unit “will provide a central hub for expert advice and legal guidance regarding the criminal electronic surveillance statutes for both U.S. and international law enforcement conducting complex cyber investigations to ensure that the powerful law enforcement tools are effectively used to bring the perpetrators to justice while also protecting the privacy of every day Americans.” The unit, which will be housed in the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division,<sup>2</sup> will work closely with law enforcement, the private sector, and Congress.

Ms. Caldwell underscored the importance of working closely with the private sector on cybersecurity issues. She indicated that the new unit “will be engaging in extensive outreach to facilitate cooperative relationships with our private sector partners” as the government “cannot and will not wage” the battle alone. She also hopes to have a larger public discussion to promote a better understanding of the role of privacy in criminal investigations. Ms. Caldwell highlighted the recent example of public outreach in which the DOJ provided a white paper to address uncertainty on the issue of whether the Stored Communications Act<sup>3</sup> bars communications service providers “from voluntarily disclosing ‘aggregate’ non-content information to the government.”<sup>4</sup> In sum, the white paper concluded that “many of the characteristics of cyber threats can be shared, if they do not pertain to any specific customers or subscribers.”

### Practical Implications

In the face of daily reports of significant hacking and computer intrusions, the new Cybersecurity Unit is an encouraging development on several fronts. First, the unit will be able to take a broad view on cybersecurity matters across enforcement and public policy areas. As an example, lessons learned on enforcement matters may lead to, or may better inform, public policy and legislative proposals.

Second, the unit is placed within CCIPS, which has a strong track record in addressing computer crime and

---

1. Leslie R. Caldwell, Ass't Att'y Gen., Criminal Div., *Cybercrime 2020: The Future of Online Crime and Investigations*, Georgetown University Law Center (Dec. 4, 2014), available at <http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-cybercrime-2020-symposium>.

2. See generally United States Attorneys' Manual (USAM) § 9-50.103 (Computer Crime & Intellectual Property Section), available at [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/50mcrim.htm#9-50.103](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/50mcrim.htm#9-50.103).

3. 18 U.S.C. §§ 2701 *et seq.*

4. Sharing Cyberthreat Information Under 18 USC § 2702(a)(3), DOJ White Paper (May 9, 2014), available at <http://www.justice.gov/criminal/cybercrime/docs/guidance-for-ecpa-issue-5-9-2014.pdf>.

# Morgan Lewis

intellectual property issues since the 1990s. Given CCIPS's history and background on these matters, it is an ideal section for the new unit in the DOJ's Criminal Division. Among other matters, CCIPS has provided leadership and guidance to federal prosecutors through the years on the collection of electronic evidence. CCIPS trial attorneys have supported and worked with Computer Hacking and Intellectual Property (CHIP) prosecutors on significant computer intrusion and intellectual property issues and matters. CCIPS has also worked closely with the National Advocacy Center on the training of federal prosecutors, among other duties and accomplishments. The leadership of the new unit on cybersecurity issues will fit nicely into the existing framework and channels used to support and provide guidance within the DOJ. By assisting more than 270 CHIP prosecutors in the CHIP Network, CCIPS learns of emerging cyber issues across the country.

Third, the speech reinforces the role of information sharing between the government and private sector. Information sharing is increasingly recognized as an essential component of an effective cybersecurity strategy.<sup>5</sup> Recent government reports have highlighted information sharing as necessary to protect against cyber threats.<sup>5</sup> Congress has also been debating legislation to promote information sharing.<sup>6</sup>

Fourth, a public debate and understanding about the role of law enforcement on privacy issues is welcome. As the speech recognizes, a key cornerstone of this understanding is based on trust. While prosecutors and agents work to solve crimes and try to make victims whole, the public would benefit from a better understanding about how law enforcement tools are employed and the checks and balances that are used in the criminal justice process.

There are a few unanswered questions from the speech: Who will lead the unit? How many prosecutors will serve in the unit? Will new resources and prosecutors be dedicated to the significant objectives and tasks charged to the unit? Although it remains to be seen what leadership and guidance will come from the new unit, the announcement is an encouraging first step that demonstrates the government's commitment to a focused approach in addressing cybersecurity.

## Contacts

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis lawyers:

### Washington, D.C./Silicon Valley

Mark L. Krotoski	+1.202.739.5024	<a href="mailto:mkrotoski@morganlewis.com">mkrotoski@morganlewis.com</a>
	+1.650.843.7212	

### Chicago

Merri Jo Gillette	+1.312.324.1134	<a href="mailto:mgillette@morganlewis.com">mgillette@morganlewis.com</a>
-------------------	-----------------	--

### Philadelphia

Greg T. Parks	+1.215.963.5170	<a href="mailto:gparks@morganlewis.com">gparks@morganlewis.com</a>
---------------	-----------------	--

### Philadelphia/New York

Barbara Murphy Melby	+1.215.963.5053	<a href="mailto:bmelby@morganlewis.com">bmelby@morganlewis.com</a>
	+1.212.309.6153	

---

5. See, e.g., Enhanced Cybersecurity Services (ECS) (a voluntary information sharing program), available at <http://www.dhs.gov/sites/default/files/publications/ECS-Fact-Sheet.pdf>; National Institute of Standards and Technology (NIST) Guide to Cyber Threat Information Sharing (Draft) (Oct. 2014), available at [http://csrc.nist.gov/publications/drafts/800-150/sp800\\_150\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf); see also Mark L. Krotoski, Brock D. Dahl, "NIST Draft Guide Advances the Debate on Cybersecurity Issues," Morgan Lewis LawFlash (Nov. 19, 2014), available at [http://www.morganlewis.com/pubs/Privacy\\_LF\\_NISTDraftAdvancesDebateonCybersecurityIssues\\_19nov14.pdf](http://www.morganlewis.com/pubs/Privacy_LF_NISTDraftAdvancesDebateonCybersecurityIssues_19nov14.pdf).

6. See Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 3523, 112th Cong., 1st Sess. (introduced Nov. 30, 2011) (passed the House by a vote of 248 to 168 on April 26, 2012); Cyber Intelligence Sharing and Protection Act of 2013 (CISPA), H.R. 624, 113th Cong., 1st Sess. (introduced Feb. 13, 2013) (passed the House by a vote of 288 to 127 on April 18, 2013); Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong., 2d Sess. (introduced July 10, 2014 and reported out by the Senate Committee on Intelligence).

# Morgan Lewis

## San Francisco

W. Reece Hirsch  
Susan D. Resley

+1.415.442.1422  
+1.415.442.1351

[rhirsch@morganlewis.com](mailto:rhirsch@morganlewis.com)  
[sresley@morganlewis.com](mailto:sresley@morganlewis.com)

## About Morgan, Lewis & Bockius LLP

Founded in 1873, Morgan Lewis offers 725 partners and nearly 2,000 lawyers—as well as scores of patent agents, benefits advisers, regulatory scientists, and other specialists—in 28 offices across North America, Europe, Asia, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. For more information about Morgan Lewis or its practices, please visit us online at [www.morganlewis.com](http://www.morganlewis.com).

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered **Attorney Advertising** in some jurisdictions. Please note that the prior results discussed in the material do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change. © 2014 Morgan, Lewis & Bockius LLP. All Rights Reserved.