CROSS-BORDER DATA ACCESS AND ACTIVE CYBER DEFENSE: ASSESSING LEGISLATIVE OPTIONS FOR A NEW INTERNATIONAL CYBERSECURITY RULEBOOK

Chris Cook*

With the ceaseless headlines about cyber-attacks against both private industry and governments, and the especially wide-reaching data breach of Equifax as well as the hacking of the American election in 2016, there is a growing discussion regarding what to do about the cybersecurity problem in America. Members in Congress are now actively debating 'hack back' authority. A bill in Congress, known as the Active Cyber Defense Certainty Act (ACDC) (H.R. 4036) would, in essence, allow private entities to go into networks outside of their own to gather intelligence and do research on unauthorized intruders to determine who is responsible for a cyber-penetration and how it occurred. While it is understandable that legislators and the public are debating the feasibility of this type of tactic, the real question is what price would the U.S. pay in exchange for deploying this capability?

This paper discusses the problems associated with 'hacking back' and with the current legislative proposal in particular. It begins with a conceptual discussion about active cyber defense, and provides a legal background explaining various theories for why certain active cyber defense tactics may or may not be lawful. The paper then then analyzes ACDC specifically, and emphasizes the definitional ambiguity in the bill, its problems with oversight

---

* Chris Cook is an attorney at the U.S. Department of Justice, National Security Division and a reserve officer with the U.S. Navy Judge Advocate General's (JAG) Corps. Prior to joining the Justice Department, Cook practiced intelligence, cybersecurity and information assurance law with the Office of General Counsel at the National Security Agency.

Author's Note: A portion of this paper appeared in an article at *Just Security* on November 20, 2017. The article, "Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act", may be found here: https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act.

All statements of fact, opinion, or analysis expressed are the author's alone and do not necessarily reflect the official positions or views of the Department of Justice or any other U.S. government agency. This article has been reviewed by the Department of Justice to prevent the disclosure of classified or otherwise sensitive information.

mechanisms, its failure to address other laws prohibiting hack back, and also the policy and strategic peril the bill introduces, particularly as it relates to international norms.

Given these concerns, the paper asks whether there are other legislative and policy options Congress should be considering with regards to cybersecurity. The paper argues that the recently enacted CLOUD Act, which deals with cross-border data access and mutual legal assistance reform, is underappreciated as a piece of cybersecurity legislation. It argues that successfully addressing data access between allies more broadly, can help facilitate more efficient international cyber investigations where electronic data is involved.

The paper outlines how the previous legal construct, prior to the CLOUD Act's enactment, was outdated, and it discusses why cross-border data access reform was necessary given the previous inefficiencies. The paper explains why the final version of the CLOUD Act successfully addressed the most strident privacy and civil liberties concerns, and argues that successful implementation of the CLOUD Act (which should be the focus going forward) may prove to be a less problematic way of attacking the attribution problem than ACDC, will help set the international norm we seek to establish in cyberspace, and could, if executed properly along with other cybersecurity advancements, be a more helpful strategic deterrence mechanism over the long-term.

INTRODUCTION.....206
I. ACTIVE CYBER DEFENSE: CONCEPTUAL FRAMEWORK.....209
II. THE LEGAL BACKGROUND.....211
A. U.S. Law.....211
B. International Law.....213
C. The Laws of Other Countries.....215
III. THE ACTIVE CYBER DEFENSE CERTAINTY ACT - ACDC (H.R. 4036).....215
A. Definitional and other Language Ambiguity.....216
B. Insufficient Liability Protection.....218
C. Uncertainty under International Law, Potential Unwanted Escalation, and the Breakdown of International Norms.....220
IV. CROSS-BORDER DATA ACCESS REFORM: A POTENTIAL LEGISLATIVE ALTERNATIVE.....221
A. The Stored Communications Act and the Problem of Cross-Border Access to Data.....222
B. The Microsoft-Ireland Case.....223
C. What Was at Stake and Why There Was a Need for Legal Reform.....224
V. THE CLARIFYING LAWFUL OVERSEAS USE OF DATA (CLOUD) ACT.....226
A. Important Protections Included in the New Legislation.....228
VI. WHY CROSS-BORDER DATA ACCESS REFORM IS A BETTER LEGISLATIVE OPTION TO ADDRESS CYBER THREATS THAN ACDC.....231
CONCLUSION.....234

INTRODUCTION

The cyber threat against the United States is real and growing. In the last few years alone, Sony, Google, JP Morgan, Target, Yahoo, and countless

others have suffered serious hacks.[1] This past summer, the ransomware known as WannaCry showed how computer code can shut down industries and cripple their ability to provide basic services.[2] The breach of Equifax, a credit reporting agency that holds the social security numbers and other personal information of more than 140 million Americans, has fueled a conversation about how to respond.[3] Increasingly, private entities are asking for the authority to defend themselves, the public is calling for action, and members of Congress have begun debating the issue of active cyber defense and "hacking back" on networks where hostile cyber activity originates. On October 13th, 2017, Representatives Tom Graves (R-GA) and Kyrsten Sinema (D-AZ) introduced a bill that would allow private entities to defend themselves by breaching the computer networks of their attackers.[4] The proposal is known as the Active Cyber Defense Certainty Act, or ACDC (H.R. 4036). While few doubt the severity of the threat, there must also be serious discussion about the implications of this proposal if enacted.

The law currently bans "hacking back." Should the United States enable the private sector to defend itself and change the law? If so, how? If not, what can we expect going forward and are there things that Congress can do besides enable "hack back" that could bolster the defense of the America's private sector against hostile cyber actors?

Active cyber defense, and ACDC more specifically, involves a spectrum of capabilities that seeks to help American companies identify their hackers. The proposal would allow private companies (and individuals) to go into foreign networks to gather intelligence and do research on unauthorized intruders and determine who is responsible and how the penetration occurred. A key question is whether this legislation would incentivize entities from other countries to do the same thing against our own networks, potentially making an already serious problem worse. Additionally, there are key questions about whether this proposal would be consistent with the rules and norms we seek to establish on the cyber battlefield. If strengthening attribution capabilities, enhancing cyber investigations, and gaining access to data from systems primarily based overseas is at the core of ACDC, there are other policy options besides "hacking back" that may help with this problem.

Another piece of legislation, enacted into law in early 2018 addresses these issues. The legislation is known as the Clarifying Lawful Overseas Use of Data

---

1. Taylor Armerding, *The 17 Biggest Data Breaches of the 21st Century*, CSO (Jan. 26, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

2. Alexander Smith et al., *Why WannaCry Malware Caused Chaos for National Health Services*, NBC NEWS (May 17, 2017), https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126.

3. Kathleen Pender, *Equifax Hack Must Prompt Lawmakers to Act*, S.F. CHRONICLE (Sept. 11, 2017), http://www.sfchronicle.com/business/networth/article/Equifax-hack-must-prompt-lawmakers-to-act-12189839.php.

4. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

(CLOUD) Act,[5] which codifies the main framework of a similar earlier proposal by the U.S. Department of Justice to address what is known as the cross-border data access problem.[6] The legislation paves the way for bi-lateral agreements between countries that would allow law enforcement to access computer data (in furtherance of cyber as well as other investigations) that is stored on foreign soil so long as certain criteria are met and agreed upon by allied nations. Though the exact limits of such agreements are still being developed and debated, there is broad consensus that cross-border investigations involving data stored abroad and the process by which those investigations are facilitated needs reform.[7] The CLOUD Act sets the framework by which these executive agreements will be structured, and in sum, substantially improves upon the cross-border data access problem.

This paper will discuss these legislative pieces, which both sit at a fascinating cross-section of criminal law, cybersecurity, data privacy, the Fourth Amendment, international law, private industry, foreign relations and national security. It will begin by discussing "hacking back" and active cyber defense as a concept, and illustrate how active cyber defense involves a spectrum of cyber defense capabilities. It will then discuss the legal background surrounding "hack back" authority, and show how the law, as currently written, prohibits most of the active cyber defense measures and "hack back" tactics being discussed today. The paper will then show how the current legislative proposal, ACDC, fails to address the law prohibiting "hacking back." It will also show how, from a policy perspective, enabling such activity is ripe with hazards, in particular as it relates to the American interest in establishing international norms to discourage private entities and individuals from unlawfully accessing computer networks overseas.

Alternatively, the paper will then discuss the CLOUD Act, which can also help with cyber attribution when such crimes involve digital evidence held abroad. The paper will illustrate how the legal landscape prior to the enactment of the CLOUD Act was a problem for American law enforcement seeking access to computer data held across international borders, and why foreign governments were similarly frustrated with pre-existing law. It will outline how successful implementation of the CLOUD Act can facilitate access to data across borders and can help solve some of the most significant crimes of our

---

5. *See* STAFF OF S. COMM., 115TH CONG., CONSOLIDATED APPROPRIATIONS ACT (Comm. Print 2018).

6. U.S. DEP'T OF JUSTICE, OFFICE OF LEGISLATIVE AFFAIRS, LEGISLATION TO PERMIT THE SECURE AND PRIVACY-PROTECTIVE EXCHANGE OF ELECTRONIC DATA FOR THE PURPOSES OF COMBATING SERIOUS CRIME INCLUDING TERRORISM (2016), https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p4.

7. *See, e.g.*, RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, (2013), https://perma.cc/C4RA-NYL8; Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC. J. (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age.

age, such as hacking. It will argue that unlike ACDC, the CLOUD Act strengthens international norms and agreements with regards to cyber-crime. Along the same lines, it will argue that it is less clear how helpful "hacking back" will be than it is clear that it introduces a myriad of complex legal, policy and strategic issues, particularly if the United States continues to advocate for a rules-based international order. The paper will show how the CLOUD Act is underappreciated as a cybersecurity proposal and how its basic framework for revising cross-border data access is a less problematic way of attacking the attribution problem, will help set the international norm we seek to establish in cyberspace, and could, if implemented properly along with other cybersecurity advancements, be a more helpful strategic deterrence mechanism over the long-term.

I. ACTIVE CYBER DEFENSE: CONCEPTUAL FRAMEWORK

The term "hack back" can be misleading. Active cyber defense can entail a spectrum of capabilities that organizations can use to defend themselves against hostile cyber activity, any number of which could fall short of "hacking back." In October of 2016, George Washington University's Center for Cyber and Homeland Security assembled a task force on the issue and published a report on its conclusions.[8] The participants on the taskforce included a wide-range of experts in government, academia, and the private sector. Task force co-chairs included retired Admiral Dennis C. Blair, the Former Director of National Intelligence, and Secretary Michael Chertoff, the Former Secretary of Homeland Security. The detailed study offered the following definition of active defense:

> Active defense is a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors. The term active defense is not synonymous with "hacking back" and the two should not be used interchangeably.[9]

The Center arrived at this definition after looking at activities that fall across the range of actions that cyber defenders can use on their own networks and on the networks of the attacker. On one end of the spectrum are activities that produce effects solely within an actor's own networks. These low-risk

8. Dennis C. Blair et al., THE GEORGE WASHINGTON UNIVERSITY, CENTER FOR CYBER & HOMELAND SECURITY, *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats* (2016), https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

9. *Id.* at xi.

options include defensive measures such as information sharing and the use of honeypots or tarpits (techniques that serve as decoys for attackers and allow the defender to observe attack techniques to inform defenses). These activities are characterized as potentially insufficient by themselves to defend against the most advanced cyber aggressors.[10] On the other end of the spectrum are activities that occur outside the actor's network, and are aimed at coercing the aggressor, imposing costs, degrading capabilities, or accessing protected information without authorization. The report characterizes these activities as "offensive."[11] Examples of this type of offensive activity could include "hacking back" to retrieve stolen data, or to retaliate with malware to damage an intruding system or even steal intellectual property. The report states that private sector actors should not be authorized to use these tactics except in very limited circumstances in cooperation with or under the delegated authority of a national government.[12] The report goes on to argue however, that there exists a "gray zone" between these two ends of the spectrum that fall between the upper and lower definitional boundaries, and proposes that there are a number of other, less controversial active cyber defense methods and tactics that should be authorized under appropriate circumstances.[13] "Gray zone" activities are moderate- to high-risk operations and generally occur outside of a defender's networks, with the potential to cause minor collateral damage or privacy concerns if used imprecisely.[14]

A prime example of "gray zone" activity would likely involve some type of intelligence gathering on an attacker's network or a type of rescue mission to recover stolen assets. While this type of activity is still legally impermissible if it were to be conducted outside a defender's own systems, the report advocates clarifying the law surrounding this type of activity and legalizing it in appropriate circumstances, i.e. when it is done with close cooperation between government and the private sector.[15] As an example of how this could work, the report cites Google's response to Operation Aurora (christened by the security firm McAfee), which was a Chinese-linked hacking campaign that went after Google's source code.[16] Google's leadership decided that it had the ability to take on a nation state and operate outside its network to track down the attackers. Google found that the attackers were controlled from, and operating in China and afterwards shared information with law enforcement, the Intelligence Community, and the public. The U.S. government did not take

10. *Id.* at 9.
11. *Id.* at 9.
12. *Id.* at 9.
13. *Id.* at 9-15.
14. *Id.* at 12.
15. *Id.* at 23-29.
16. *See* Kim Zetter, *Google Hack Attack Was Ultra Sophisticated, New Details Show*, WIRED MAG. (Jan. 14, 2010), http://www.wired.com/2010/01/operation-aurora.

legal action against Google and instead rebuked China while praising the tech giant.[17]

The law as currently written does not authorize individuals, or organizations to access networks outside of their own without consent, even if they are clearly being attacked from that network. As discussed below, it can be a criminal violation to access a computer without authorization. Google, therefore, took significant risks by undertaking this operation. However, Google is not the only company that has calculated that this is a risk worth taking in the right circumstances, and other private organizations have been reported to undertake similar activity.[18] The Center for Cyber & Homeland Security, and other commentators, see the Google case, and other similar cases where private organizations have taken limited steps to defend themselves as an example of how this could work going forward.[19] Provided these types of actions are done with legal authorization and are not destructive, the assumption is that this type of limited active cyber defense might be sustainable, technically and politically. However, these kinds of operations would not be risk-free. Any proposal authorizing such operations would need stringent boundaries and oversight mechanisms, and there would need to be changes in the law to enable it.

II. THE LEGAL BACKGROUND

A. *U.S. Law*

Currently, there is no explicit right of self-defense by private companies against cyber threat actors in domestic or international law. The main statutory limitations against such activity are codified under the Computer Fraud and Abuse Act (CFAA), the Wiretap Act, The Electronic Communications Privacy Act (ECPA), and the federal prohibition on Pen Register Trap and Trace (PRTT) devices. There are broad similarities in these statutes as they pertain to hacking. All prohibit, in some form, unauthorized access and/or collecting or intercepting data on a system outside of one's own.

The most often cited "anti-hacking" statute in the United States is the CFAA (18 U.S.C. § 1030 *et seq*).[20] The CFAA makes it illegal for anyone who

17. BLAIR ET AL., *supra* note 8, at 13-15.

18. *See* Michael Riley & Jordan Roberson, *FBI Probes If Banks Hacked Back as Firms Mull Offensives*, BLOOMBERG (Dec. 30, 2014), http://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives.

19. *See* William Roth, *Deputizing private sector cybersecurity firms to fight cyber crime*, SASAKAWA USA (Sept. 26, 2016), https://spfusa.org/sasakawa-blog/deputing-private-sector-cybersecurity-firms (drawing an analogy between licensed cybersecurity firms authorized to engage in limited intelligence gathering techniques on external networks and U.S. State licensure of railroad police of limited powers in situations where government is incapable of keeping the peace).

20. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008).

a) Accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer; b) Knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; c) Intentionally accesses a protected computer without authorization, and as a result of such conduct recklessly cause damage; or d) Intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss.[21]

Most of the more forceful cyber defense measures discussed above would likely be in violation of this law. For instance, an active cyber defense measure that goes outside one's own network to retrieve, alter or erase stolen data, or to disrupt an attack through malware, or even damage an attacking computer would require unauthorized access to that computer. Moreover, less extreme measures such as observation, beaconing, and monitoring, could still be problematic if conducted outside one's own network because it would involve unauthorized access to data on another computer.

There are similar limitations under the Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2510 -22)[22] – Pen Register/Trap and Trace statute (PRTT) (18 U.S.C. § 3121-27)[23] and the Wiretap Act (18 U.S.C. § 2510 *et seq*).[24] The relevant provisions of the Wiretap Act make it illegal for anyone to intentionally or purposefully intercept (or endeavor to intercept), disclose or use the contents of any wire, oral, or electronic communication. Thus, certain cyber defense tactics may be in violation of the Wiretap Act in addition to the CFAA. For example, the use of honeypots or sink-holing to intercept malicious traffic could be considered an intercept of an electronic communication. Furthermore, under the Pen Register/Trap and Trace statute, it is illegal for anyone to install a pen register or trap and trace device (a device that captures dialing, routing, addressing, or signaling information) without obtaining a court order.[25] Thus, the PRTT statute may also apply to any technique that involves capturing incoming intruder data.

There are various theories for how the main statutory limitations can be overcome through existing law. For instance, the Wiretap Act has an exception that allows law enforcement officials to monitor and investigate the activity of hackers under certain circumstances, i.e. when they have consent of the owner of the victim network or an order has been issued upon a showing of probable cause.[26] There is also some ambiguity about the meaning of "authorization" under the CFAA, or "exceeds without authorized access" in various case law,

---

21. *Id.*

22. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22 (2002).

23. Federal Prohibition on Pen Register Trap and Trace Devices, 18 U.S.C. § 3121 (2001).

24. Wiretap Act, 18 U.S.C. § 2510 (2002).

25. 18 U.S.C. § 3121 (2004).

26. 18 U.S.C. § 2518 (1998).

as well as arguments that the CFAA is vague and overbroad.[27] There are also arguments under common law theories of trespass where under certain circumstances, one can interfere with another's personal property to defend his or her own personal property.[28]

The full scope of these common law theories and other exceptions to the statutory framework is beyond the scope of this paper. However, it is useful background for understanding the domestic legal landscape. There are also similar limitations and restrictions under international law.

B. *International Law*

There is no overarching international law that specifically addresses active cyber defense by private actors.[29] The vast majority of international law focuses on nation-states and their actions. For example, the main body of international law, the U.N. Charter, discusses nations' rights to self-defense, but not that of private actors.[30] The Tallinn Manual, an academic, non-binding study of international law as it applies to cyber conflict, is similarly limited to nation state actors, and does not discuss private sector cyber defense.[31] The recently published Tallin Manual 2.0 addresses hostile cyber activity (including such activity conducted by non-state actors) that falls below the international law thresholds of "armed attack" and "use of force," but its rules are focused on what state actors can do in response to this activity, and does not get into a detailed discussion about what private actors may do in these circumstances.[32]

Paul Rosenzweig, a professor of law at George Washington University, and frequent commentator on cyber law, notes that the Budapest Convention on CyberCrime is perhaps the most directly relevant international instrument that discusses cyber self-defense issues.[33] Rosenzweig notes that the accompanying 2001 Explanatory Report to the Budapest Convention anticipates the idea that signatory parties should criminalize certain actions, but that parties are free to defend themselves and establish legal remedies, excuses, or justifications for such defensive actions.[34] It may be a stretch to interpret the Convention to

---

27. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562 (2010).

28. *See* Stewart Baker, Orin Kerr & Eugene Volokh, *The Hackback Debate*, STEPTOE CYBER BLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate.

29. *See* Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. OF INT'L L., 103, 108 (2014).

30. U.N. Charter art. 51., ch. VII.

31. THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., Cambridge Univ. Press 2013).

32. THE TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., Cambridge Univ. Press 2017).

33. Rosenzweig, *supra* note 29.

34. *Id.*; *see also* COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME (2001), https://rm.coe.int/16800cce5b.

mean that certain aggressive active cyber defense measures would be lawful, but the notion is at least considered.

One area of international law that has gained a great deal of attention in the academic literature surrounding this topic is the law of piracy, and more directly, the law of 'privateering'.

There are a number of striking similarities between the issues of piracy and the modern-day cybersecurity threat environment. The ocean serves a similar function as the internet does today in its transfer and flow of goods. Hackers have been likened to pirates in the sense that they are both in the business of stealing property, intellectual or physical. Various proposals today seek to implement the lessons learned from the modern-day piracy problem and transfer them to the cybersecurity environment.[35] The analogy is helpful for conceptualization of the problem, but there are also serious limits to the historical parallel.[36]

These limits can be seen both from a legal and a strategic policy perspective. Under maritime rules, merchantmen were entitled to use self-defense to repel pirates, but only state-owned vessels were given the authority to board and seize a pirate ship or engage in hot pursuit.[37] Critically, the right to pursue ended when the pirate ship entered the territorial waters of another country. Companies today seeking to "hack back" to protect their stolen data would have to cross territorial lines to do so. Therefore, if aggressive cyber countermeasures by the private sector are intended to be used in countries and on networks where the hostile cyber activity originates, the analogy is less useful.[38]

To get around the issue of state-ownership and hot pursuit however, many argue that cyber "letters of marque" or some form of privateering or lawful deputizing of private entities is appropriate.[39] However, this is also not a clean parallel.[40] Generally speaking, privateering to combat piracy was only authorized during a time of war. Whether the same rules apply where there is no ongoing armed conflict is not clear. Even outside armed conflict, pirates are

35. Through the mid 2000's, piracy off the coast of Somalia was a vexing problem even for powerful navies. The addition of armed security on shipping vessels, however, seems to have been the tipping point where modern-day Somali piracy diminished to much more containable levels. As evidence of this phenomenon, proponents of such a policy are able to point to an incredible statistic: attacks by Somali pirates in the Gulf of Aden declined from a peak of 237 in 2011 to zero in 2015 (after private armed security guards were introduced), and only two attempts in 2016. *See* Hoffman, Wyatt, and Levite, Ariel E., PRIVATE SECTOR CYBER DEFENSE: CAN ACTIVE MEASURES HELP STABILIZE CYBERSPACE?, *Carnegie Endowment for International Peace*, 2017.

36. *See* Florian Egloff, *Cybersecurity and the Age of Privateering: A Historical Analogy*, UNIVERSITY OF OXFORD CYBER STUDIES PROGRAMME (Working Paper, Mar. 2015).

37. Rosenzweig, *supra* note 29, at 110.

38. *Id.*

39. *See* Dave Aitel, *Cyber Deterrence "At Scale,"* LAWFARE (June 10, 2016, 8:51 AM), https://www.lawfareblog.com/cyber-deterrence-scale.

40. *See* Egloff, *supra* note 36.

also, for the most part, easy to identify on the high seas once they have commenced criminal activity. Cyber actors, by comparison, are better able to obfuscate their activity and hide who may be responsible for the criminal action.[41]

There are also international conventions against privateering that may or may not carry forward when applied to cyber activity.[42] Depending on the scope of what is being proposed, active cyber defense would likely require an international agreement of some kind to build a consensus for such activity.

C. *The Laws of Other Countries*

The need to build international consensus or understanding on this issue exists because hacking into foreign networks—even to only gather intelligence—would be breaking other countries' laws in addition to our own. Most countries around the world have similar statutory and legal frameworks prohibiting "hacking back" just as we do.[43]

However, other countries have suffered devastating hacks, and they are similarly debating response options. While there are various proposals around the world regarding active cyber defense, what the scope of these national policies are and where they stand today across the board are far from uniform.[44] To the extent that U.S. actors would be probing the networks of hackers located in other countries, it would be prudent to consider that domestic actions may be perceived differently in countries where such effects may be felt. Other countries may interpret U.S. private companies using active cyber defense measures as fully sanctioned U.S. government actions and may impute state responsibility to such activity. Under these circumstances, there may be several possible avenues for retaliation if the law were to change without building a consensus among other nations beforehand.

It is worth looking at the current proposal in-depth to see how the legal and policy issues outlined above are addressed.

III. THE ACTIVE CYBER DEFENSE CERTAINTY ACT - ACDC (H.R. 4036)

For years now, there has been a discussion surrounding the feasibility of active cyber defense, and "hacking back," but there has not been a major push in Congress to explicitly authorize such activity, or to propose

41. *Id.*

42. *See* Convention on the High Seas art. 19, Apr. 29, 1958, 450 U.N.T.S 11.

43. For example, Germany's prohibition on hacking is contained in what is known as the "The Hacker Paragraph" which can be found in section 202a of the German Criminal Code. STRAFGESETZBUCHES, STGB CRIMINAL CODE, § 202a, para. 1, *translation at*, http://www.gesetze-im-internet.de/englisch_stgb.

44. *See* Robert S. Dewar, *Zurich Center for Security Studies, Cyber Defence Trend Analysis 1: Active Cyber Defense*, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-03.pdf.

changes/exceptions under the current legal and statutory framework to enable it. This looks to be changing with the proposal introduced by Representatives Tom Graves (R-GA), Kyrsten Sinema (D-AZ) and the Active Cyber Defense Certainty Act (H.R. 4036). The legislation provides an exception to liability under the Computer Fraud and Abuse Act and, in essence, would authorize individuals or organizations to go into networks outside of their own to gather intelligence on hackers for attributional purposes.[45] There are significant concerns with this legislation.

First, the bill contains a large amount of linguistic ambiguity that may in fact defeat the purpose of the legislation entirely. Second, the bill provides insufficient legal protection for would-be defenders. The bill lacks civil liability protection, does not exempt users from prosecution, and only addresses the CFAA and not the electronic surveillance statutes such as the Wiretap Act and ECPA. Third, the legislation does not account for the lack of consensus under international law for this type of activity, does not adequately guard against unwanted escalation, and perhaps most importantly, breaks down the international norm against hacking that the U.S. has strongly advocated for years. Each of these concerns is examined in-depth below.

A. *Definitional and other Language Ambiguity*

The text provides at Section 4 (1) that "It is a defense to a criminal prosecution under this section that the conduct constituting the offense was an active cyber defense measure." The term "active cyber defense measure" is defined as any measure "(I) undertaken by, or at the direction of a defender; and (II) consisting of accessing without authorization the computer of the attacker to the defender's own network to gather information in order to – (aa) establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity; (bb) disrupt continued unauthorized activity against the defender's own network; or (cc) monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques."[46]

The term "defender" is defined as "a person or an entity that is a victim of a *persistent* unauthorized intrusion of the individual entity's computer."[47] As Robert Chesney at the University of Texas and Herb Lin at Stanford have noted, the word "persistent" is probably an effort to prevent invocation of ACDC by one who has experienced only a nuisance on their computer network, however the word "persistent" is not precise either.[48] As Chesney noted, it

45. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

46. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

47. *Id.* (emphasis added).

48. Robert Chesney, *Legislative Hackback: Notes on the Active Cyber Defense Certainty Act Discussion Draft,* LAWFARE (Mar. 7, 2017), https://lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft; *see also* Lin

could refer to the time on a network in relation to a particular intrusion, or to a series of intrusions, or both, but we do not know what is enough to count as *persistent*. If an "attacker" bounces on and off a network over a period of time, does this count as persistent? A defender cannot know for certain if they can actually take advantage of the bill's provisions. The term itself leaves room for interpretation.

The text defines the term "attacker" as "a person or an entity that is the source of the persistent unauthorized intrusion into the victim's computer." However, the text does not define what the "*computer* of the attacker" is. Chesney and Lin also had concerns with this language and previously noted that often times there is more than one computer in an attack chain.[49] If there are multiple computers involved in an intrusion, it can be difficult to determine its source. The updated version of the bill defines an "intermediary computer" as "a person or entity's computer that is not under the ownership or primary control of the attacker but has been used to launch or obscure the origin of the persistent cyber-attack." Nonetheless, it can still be difficult to decipher when such intermediary computers are under the control or ownership of the attacker. An "intrusion" on an intermediary computer can sometimes be brief. Hostile cyber actors can bounce on and off networks at will, sometimes using a network as a hop point before infiltrating other systems.

This can be a problem for individuals and organizations who are considering the use of these tools against intermediary computers. For instance, the bill provides exceptions to liability protection when the defender does things that are explicitly listed as outside the definitional boundaries of "Active Cyber Defense" measures. For instance, Active Cyber Defense measures does not include conduct that (IV) intentionally exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion; or (V) intentionally results in intrusive or remote access into an intermediary's computer.[50]

This is clearly an effort to limit the potential damage to innocent "intermediary computers", but reading (IV) and (V) together can also leave room for interpretation and confusion. Part (IV) is an attempt to set a precise limitation that access on an intermediary computer can only be for reconnaissance and attribution purposes, but how can a defender know if, pursuant to part (V), their action does not intentionally result in intrusive or remote access into such a computer? Does the word *intrusive* essentially mean "without permission?" We also do not know what constitutes remote access. If (V) prevents intrusive and remote access on an intermediary computer, does it effectively require users of active cyber defense measures to get the consent of owners of intermediary computer networks before doing attributional

& Herb, *More on the Active Cyber Defense Certainty Act*, LAWFARE (Mar. 24, 2017), https://www.lawfareblog.com/more-active-defense-certainty-act.

49. *Id.*

50. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

reconnaissance? Computer network owners are unlikely to consent to outside actors getting onto their networks, even if it is ostensibly for defensive purposes. Therefore, if getting such consent is unlikely, it may defeat the purpose of the legislation entirely.

The inclusion of the word *intentionally* in (IV) and (V) is also an update from previous drafts. The drafters likely sought to include this word to give defenders an added layer of assurance that their particular state of mind would be taken into account when determining whether liability protections apply. However, as Andrea Little Limbago, the chief social scientist at the cyber security firm Endgame has noted, by adding this layer of assurance, the drafters have actually expanded the scope of what a defender can do on an attacker's network.[51] If it is a defense against liability for a defender to assert that they did not intend certain effects of their actions, a defender is more likely to take risks. The result is that the drafters may have inadvertently increased the risks of escalation by including this language. Moreover, there is a good chance that defenders will use active cyber defense measures against the wrong attacker or computer. This would be especially true when the parties have asymmetric experience and capacity, such as a novice defender responding against sophisticated cyber actors who have spent years developing deceptions within their attack code.[52]

There are other listed exceptions to liability protection, such as when a defender "creates a threat to the public health or safety" or when a defender's action "intentionally results in the persistent disruption to a person or entities internet connectivity . . ." These and other exceptions are good-faith efforts to limit the very real collateral damage concerns that can arise in "hacking back," but there is still very little clarifying language about what these terms actually mean. The bill does not elaborate on what constitutes a threat to public health or safety, or what a persistent disruption is.

B. *Insufficient Liability Protection*

Critically, the bill also states that use of "active cyber defense measures" is a "defense" to criminal prosecution. But proponents of active defense are seeking authorization and total exemption from prosecution for taking defensive action. An affirmative defense will still permit the government to charge private parties with violating the CFAA and will require those parties to submit to litigation and to satisfy the affirmative defense before being exonerated. There is also a reminder in the bill that liability protection only extends to criminal prosecution. The bill explicitly states that "the defense against prosecution in this section does not prevent a United States Person or

51. Andrea Little Limbago, *The Hacking Back Bill Isn't the Answer to Cyberattacks*, WAR ON THE ROCKS (Oct. 31, 2017), https://warontherocks.com/2017/10/the-hacking-back-bill-isnt-the-solution-to-cyberattacks.

52. *Id.*

entity who is targeted by an active defense measure from seeking a civil remedy, including compensatory damages or injunctive relief . . .” This is an ominous cue that lawyers for companies or individuals seeking to use such measures would highlight very plainly. The bill also says nothing about state laws, many of which have similar prohibitions against hacking.

Also, the bill only amends the CFAA and says nothing about the electronic surveillance statutes such as the Wiretap Act, the Electronic Communications Privacy Act, and the Pen Register Trap and Trace statute. Because ACDC measures would likely involve infiltration and/or monitoring of an attacker’s network, such techniques would likely fall under the category of electronic surveillance, and violate these other important federal laws. The bottom line is that it is not abundantly clear to a defender looking to use these techniques that they are not taking on undue legal risk.

There is, however, new language in the latest proposal that includes a voluntary pre-emptive review by the Federal Bureau of Investigation (FBI) before using ACD measures, which is a good step in alleviating these concerns.[53] But it does not go very far. All that is required under the current proposal is that users of ACD measures must notify FBI of their intent to use such techniques. The pre-emptive review itself and actually getting the FBI’s permission to take specified action is voluntary. Individuals and organizations are unlikely to wait for the formal blessing of the FBI, or in some cases may exceed what was previously authorized given the nature of an intrusion and unforeseen developments related to it. Given the likelihood of unwanted second and third order effects when using these types of countermeasures, there is thus a great deal of danger that liability protections will not apply the way they are intended.

Additionally, as far as oversight is concerned, the draft proposal says very little. The language regarding the voluntary FBI pre-emptive review effectively requires the FBI-led National Cyber Investigative Joint Task Force to build and set its own internal procedures to oversee this type of program and create further guidance/feedback for users of active cyber defense measures. One of the common concerns that led to the drafting of ACDC in the first place is that government does not have the resources to defend the entire private sector in cyberspace. While the latest proposal acknowledges that the FBI may decide how to prioritize the issuance of such guidance to defenders based on the availability of resources, it still leaves room for questioning how strained will the FBI become in overseeing this type of program. Those seeking guidance and assurance that they are not outside the bounds of the law may not be able to receive it. We also do not know what the specific mechanisms of oversight and guidance would look like.

53. *See* Active Cyber Defense Certainty Act, *supra* note 4.

C. *Uncertainty under International Law, Potential Unwanted Escalation, and the Breakdown of International Norms*

There is also an ancillary concern that the FBI pre-emptive review language presents. Kristen Eichensehr of the UCLA School of Law notes that adding such language and explicitly including the FBI in the process implicates international law. "The FBI's participation in the review process may trigger the U.S. government's international legal responsibility for actions of private actors."[54] It follows that, "If the United States is responsible for international law violations committed by private actors, then international law permits aggrieved foreign governments to take countermeasures against the United States . . . ."[55] The potential for escalation is therefore substantial. The bill could actually constrain international cooperation and intensify the possibility of retaliation.

There is nothing in the draft proposal that limits what types of individuals/entities could pursue such tactics. The George Washington University's Center for Cyber and Homeland Security in its Report on this issue suggested that the U.S. might be better served by having a set number of highly skilled firms who are vetted and licensed to conduct active cyber defense.[56] The current draft effectively allows anyone, so long as their activity falls under the excepted provisions of the statute, to take on a cyber-adversary. Are we comfortable allowing any company with an IT department to take on a nation-state?

Another big concern, already mentioned above, is the lack of uniformity among nations for how active cyber defense would be perceived and accepted around the world. If active cyber defense measures are going to be used against on networks and servers outside the U.S., such actions will be subject to foreign law. "Hacking back," as mentioned, is illegal in most countries where U.S. actors would likely be operating. Under normal circumstances, the U.S. would honor an extradition request from affected nations where these types of countermeasures are expected to be deployed, absent a change in the law. If the U.S. were to ignore such requests or to change the law, foreign nations can be expected to retaliate in kind. Given the inherent vulnerabilities in our highly digitized society, this may not be strategically wise. The crucial question policy makers should be asking is whether we are comfortable allowing foreign actors/private entities do on our own networks what we are proposing to authorize on theirs.

James Lewis at the Center for Strategic and International Studies has opposed hacking back and aggressive active cyber defense in part for these

---

54. Kristen Eichensehr, *Would the United States be Responsible for Private Hacking*?, JUST SECURITY (Oct. 17, 2017), https://www.justsecurity.org/46013/united-states-responsible-private-hacking.

55. *Id.*

56. *See* Blair et al., *supra* note 8, at 23-29.

reasons. He calls the notion a "remarkably bad idea that would harm the national interest . . . and that encouraging corporations to compete with the Russian mafia or Chinese military hackers to see "who can go further in violating the law, is not a contest American companies can win."[57] The situation could very easily become complicated if and when the Chinese government, for example, catches a U.S. firm hacking back and requests an arrest warrant through Interpol for the company's CEO.[58] The U.S. is unlikely to honor such requests, but under those circumstances, Lewis questions whether cyber defenders would be willing to take on the risks of traveling abroad.[59] It is not hard to see another country, one that is not an adversary even, having similar concerns and/or make similar requests.

In the same article, Lewis also notes that allowing individuals or companies to engage in hack back would signal an abandonment of U.S. efforts to establish international norms against this type of activity.[60] Even activity that falls short of hack back, like accessing foreign networks without consent, could bring U.S. credibility to international norm building into question. For years, the U.S. has pushed the idea that unauthorized hacking is illegal, and should not be done. Enacting ACDC into law without building a consensus internationally beforehand would implicitly contradict these efforts. By allowing companies/individuals to engage in this type of activity, Lewis points out that we would no longer be able to hold others who conduct such activity to account. The rules of the cyber battlefield would be potentially be altered in ways that may not be desirable.

IV. CROSS-BORDER DATA ACCESS REFORM: A POTENTIAL LEGISLATIVE ALTERNATIVE

Given the inherent complexities that active cyber defense presents, and in particular the problems it presents with other countries, it is prudent to consider whether there are other, less controversial ways that lawmakers can help to address the cybersecurity threat. If a central purpose of ACDC is to enhance the ability to attribute hostile cyber activity, and if much of the digital evidence for unlawful hacking is often stored overseas, a newly enacted law, which may be underappreciated as it relates to cybersecurity, addresses this issue and it is one that could actually help build a more attractive international norm.

The law is known as the Clarifying Lawful Overseas Use of Data (CLOUD) Act. The law provides a fix to what is known as the cross-border data access problem. The crux of the problem is twofold. One issue is that the

57. Max Fisher, *Should the U.S. Allow Companies to 'Hack Back' Against Foreign Cyber Spies?*, WASH. POST (May 23, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/?utm_term=.4ecbc65a647b.

58. *Id.*

59. *Id.*

60. *Id.*

Stored Communications Act (SCA) (enacted prior to the CLOUD Act) prevented U.S. companies from disclosing the content of communications and other digital evidence to foreign governments. The second is that the SCA may also have prevented American companies from providing digital evidence to the U.S. government when they store their data abroad.

The CLOUD Act seeks to fix these problems. It builds upon an earlier proposal from the U.S. Department of Justice which amends the SCA and would enable approved foreign governments to enter into executive agreements with the U.S. to allow them to submit requests for electronic data directly to U.S. companies. Also under the new legislation, the U.S. would be granted reciprocal rights with foreign partner nations.

For reasons explained below, the legislation is a significant step forward on the issue of cross-border data access, and it updates the legal foundations for how nation-states conduct investigations that involve computer evidence held across the globe. The law's scope is much wider than just cybersecurity, but because of the nature of cyber-crime and digital evidence in today's environment, the importance of the law for cybersecurity is underscored. To understand how the legislation improves the legal framework, it is important to understand precisely what the problem was.

A. *The Stored Communications Act and the Problem of Cross-Border Access to Data*

When investigating cybercrime (in addition to other crimes), governments often need evidence that is held in other countries. Often, that evidence is held by U.S. tech companies. However, the Stored Communications Act (SCA), as mentioned, prohibited U.S.-based companies from turning over emails, and the content of stored communications and other digital information to foreign governments.[61] The SCA was enacted as Title II to the Electronic Communications Privacy Act, and was intended to create Fourth Amendment-like privacy protection for email and other digital communications stored on the Internet.[62]

The problem, however, is that the good intentions behind the SCA have not stood the test of time. Digital evidence is stored today in the global cloud and tech companies amass data for their customers all over the world. For instance, Microsoft, which will be discussed further below, stores data for its customers based on where that customer says they are physically located. Google breaks up its customers' data and stores pieces of digital evidence on a number of different servers throughout many different parts of the planet; other companies

61. 18 U.S.C. § 2702 (1986).

62. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislature's Guide to Amending it*, 72 GEO. WASH. L. REV. 1208, 1212 (2004).

have even more complex data storage constructs.[63] The result is that the Fourth Amendment protections sought by the bill's drafters do not apply the way they were envisioned. In earlier times, when computer data was stored almost exclusively in the United States, by American companies, the United States had unquestioned jurisdiction. Today, while some data is ostensibly controlled by U.S. companies, it "resides" on foreign soil. According to some, it may therefore be subject to foreign law.[64] There had been long-standing calls for the reform of the SCA, as legal experts, such as Orin Kerr and others, noted that its drafters could not have foreseen how the legal and technological landscape has so dramatically altered its application.[65]

Prior to the CLOUD Act's enactment, the problem with the SCA and global law enforcement investigations was apparent in two main situations, already mentioned above. The first is that it was not clear if the SCA applied extraterritorially. That is, it was not clear if the SCA prohibited American companies from producing content to the *U.S. Government* when that company had chosen to store its data abroad. The second problematic situation, is that the SCA explicitly prohibited U.S. companies from responding to *foreign* law enforcement demands for the contents of digital data, even when that data was stored on foreign soil.

These legal issues were at the forefront of a once highly anticipated case before the U.S. Supreme Court, in *Microsoft Corp. v. United States,*[66] also known as the Microsoft-Ireland case.

B. *The Microsoft-Ireland Case*

The facts of the Microsoft-Ireland case were relatively straightforward. A warrant directed Microsoft to seize and produce the contents of an e-mail account that it maintained for a customer who was using the company's electronic communications services.[67] A U.S. magistrate judge, having found that there was probable cause to believe the account was being used in furtherance of a crime, issued the warrant.[68] Microsoft produced its customer's

63. *See* Sean Gallagher, *The Great Disk Drive in the Sky: How Web Giants Store Big–and We Mean Big–Data*, ARS TECHNICA (Jan. 26, 2012, 6:00 PM), https://arstechnica.com/information-technology/2012/01/the-big-disk-drive-in-the-sky-how-the-giants-of-the-web-store-big-data.

64. *See* Br. in Opp'n to Pet. for a Writ of Cert. at 2, United States v. Microsoft, 2017 WL 3809741 (No. 17-2) (filed Aug. 28, 2017).

65. *See* Kerr, *supra* note 62, at 1213-14.

66. Robert Barnes, *Supreme Court to Consider Major Digital Privacy Case on Microsoft Email Storage*, WASH. POST (Oct. 16, 2017), https://www.washingtonpost.com/politics/courts_law/supreme-court-to-consider-major-digital-privacy-case-on-microsoft-email-storage/2017/10/16/b1e74936-b278-11e7-be94-fabb0f1e9ffb_story.html?utm_term=.b8451f1a0e41.

67. *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 201 (2d Cir. 2016).

68. *Id.* at 200.

information from data that was stored in the United States, but argued that for data held outside the United States, it was prohibited from doing so based on the specific language of the SCA, and the fact that the warrant did not carry extra-territorial authority.[69]

Microsoft's challenge to the warrant requirements went before the United States District Court for the Southern District of New York, who ruled in favor of the government. However, the case was vacated and remanded by the Second Circuit Court of Appeals who ruled in favor of Microsoft. The case was subsequently taken up by the United States Supreme Court, which held oral arguments in February, 2018. The Supreme Court took the case in the absence of a circuit split at the appellate level, indicating the importance with which the Court viewed the issues at hand. Each side viewed the stakes for this case as momentous, and argued that any decision would have far-reaching impact for law enforcement, the private sector, and the public at large. The Second Circuit opinion in the Microsoft case (as well as Judge Lynch's concurring opinion) is worth reviewing in full, as the government raised important issues that, before the CLOUD Act's passage, were to be reviewed by the Supreme Court. Ultimately, the Second Circuit concluded that Congress did not intend the SCA's warrant provisions to apply extraterritorially.[70]

C. *What Was at Stake and Why There Was a Need for Legal Reform*

The CLOUD Act's passage has rendered the Microsoft-Ireland case moot, but prior to its enactment, the case was set to have ripple effects internationally, and would have set a precedent for investigations involving cross-border data that would have been difficult to overcome. Microsoft asserted that for customers using its services, they assign servers and hosting services based on where the customer says they are located. If a customer says he is located in Ireland, as the customer was in the Microsoft case, most of the electronic data pertaining to that customer will be held in Ireland. Other companies, as mentioned, have similar or even more complex data storage frameworks. Thus, nefarious actors could take advantage of the gap in the law, as criminals, including hackers, could potentially position their data in such a way to be outside the reach of the U.S. government. The law-enforcement implications were therefore substantial. Investigators feared a ruling in favor of Microsoft could have resulted in the loss of the ability to obtain digital evidence in hundreds, if not thousands of criminal as well as national security cases, from terrorism, to child pornography, and of course, computer fraud.[71]

---

69. *Id.* at 201.

70. *Id.* at 42.

71. *See* Ellen Nakashima, *Supreme Court to Hear Microsoft Case: A Question of Law and Borders*, WASH. POST (Feb. 25, 2018), https://www.washingtonpost.com/world/national-security/supreme-court-case-centers-on-law-enforcement-access-to-data-held-overseas/2018/02/25/756f7ce8-1a2f-11e8-b2d9-08e748f892c0_story.html.

Microsoft, and many in the private sector, feared that a ruling in favor of the government would have left no basis to object when a foreign government demanded data on citizens located in the United States.[72] The private sector also feared that a ruling in favor of the government could have put the multibillion-dollar business of the global cloud in legal peril. E. Joshua Rosenkranz, who argued Microsoft's case, called the government's position "a recipe for global chaos" and asserted that ruling in favor of the government will be sure to stoke international tension and will inevitably create a conflict of laws among nations who will assert extraterritorial jurisdiction in their own investigations, or will determine U.S. companies who are forced to comply with U.S. demands for data (or prevented from responding to local demands) as being in violation of sovereign law.[73]

The lack of legal clarity surrounding the SCA forced the U.S. government and foreign governments to rely on Mutual Legal Assistance Treaties (MLAT) to get access to electronic content on the internet. However, the MLAT process had proven to be problematic in its own right. The MLAT process requires foreign governments to make a diplomatic request to the U.S. for access to evidence held in the U.S. Such requests have to be routed through the Department of Justice's Office of International Affairs and ultimately requires a U.S. Judge's approval, who bases his or her opinion on the U.S. standard of probable cause. The process was studied in depth by President Obama's Review Group in Intelligence and Communications Technologies, who determined that the lag time for such requests takes an average of about ten months.[74] Because foreign governments conducting investigations of crimes (including cyber-crimes) were increasingly asking for computer data held by U.S. companies, and because they need access to information quickly, they had grown increasingly frustrated by the MLAT process. The U.S. government was similarly frustrated by the time constraints when its own MLAT requests to foreign governments were made. The MLAT process was not built for the abundance of requests for digital evidence, which shows no signs of abating, nor was it built for changing of the technological landscape which scholars have noted makes government access to computer data ever-more challenging.[75]

As a result, governments around the world had been exploring other ways of accessing computer data outside of the MLAT process. As scholars Tiffany

---

72. *Id.*

73. *Id.*

74. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES. (2013), https://obamawhitehouse.archives.go/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

75. *See* Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, 2 INT'L DATA PRIVACY L. 200 (Nov. 2012); OHIO STATE PUB. L. WORKING PAPER NO. 175., Apr. 12, 2012.

Lin and Mailyn Fidler of Harvard's Berkman Klein Center for Internet & Society have noted in their research on cross-border data access, some of these states' methods have included expanding their own surveillance capabilities, limiting use of encryption, mandating data localization, expanding extraterritorial application of their laws, and letting law enforcement exploit software vulnerabilities.[76] All of these methods, Lin and Fidler note, are antithetical to U.S. interests, such as an open Internet, which the U.S. has historically championed.[77] The ACDC proposal in the United States can also be viewed as an outgrowth of this problem, as it seeks to address the perceived insufficiencies of traditional law enforcement methods when it comes to stolen data held abroad.

The state of the law caused virtually everyone to call for a change.[78] No one seemed happy with the previous legal construct. The debate was what a change in the law should actually look like.

V. THE CLARIFYING LAWFUL OVERSEAS USE OF DATA (CLOUD) ACT

On February 6, 2018, Senators Orrin Hatch, Christopher Coons, Lindsey Graham, and Sheldon Whitehouse introduced the CLOUD Act which was an improvement from many other previous proposals to address these issues.[79] The CLOUD Act builds upon and codifies the main framework of an earlier proposal laid out by the U.S. Department of Justice, and amends the SCA, changes the mutual legal assistance process for computer data, and moots the Microsoft-Ireland case. Remarkably, the law also has the support of the Department of Justice, as well as tech firms such as Microsoft, Google, and Facebook.[80] It also has the support of the British government, which is likely to be the first foreign government to enter into an executive agreement that the

76. Tiffany Lin & Mailyn Fidler, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y AT HARV. U, CROSS-BORDER DATA ACCESS REFORM: A PRIMER ON THE PROPOSED U.S.-U.K. AGREEMENT 4 (Sept. 13, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035563.

77. *Id.*

78. *See, e.g.*, Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC JOURNAL ONLINE (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age; PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'N TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 79 (Dec. 12, 2013) https://perma.cc/C4RA-NYL8; VIVEK KRISHNAMURTHY, CLOUDY WITH A CONFLICT OF LAWS, BERKMAN KLEIN CEN'R RESEARCH PUBL'N 1 (Feb. 18, 2016) https://ssrn.com/abstract=2733350; Cen'r for Strategic and Int'l Studies, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, (Jan. 29, 2015), http://globalnetworkinitiative.org/content/data-beyond-borders-mutual-legal-assistance-internet-age.

79. Ali Breland, *Hatch Introduces Bi-partisan Bill to Clarify Cross-Border Data Policies*, THE HILL (Feb. 6, 2018), http://thehill.com/policy/technology/372637-hatch-introduces-bipartisan-bill-to-clarify-cross-border-data-policies.

80. Tech Companies Letter of Support for Senate CLOUD Act (Feb. 6, 2018) https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.

law paves the way for in allowing foreign government access to U.S. held data.[81]

The CLOUD Act amends the SCA by adding a section at 18 U.S.C. 2713 which reads: "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber *within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States*."[82]

This language is consistent with the government's arguments in the Microsoft-Ireland case and it provides an answer to the main question that was being litigated: *The SCA applies extraterritorially*, but there are now vital requirements included that are designed to protect both foreign government sovereignty and privacy rights (more on this later). This language satisfies the U.S. government, because it would enable U.S. law enforcement access to data stored abroad.

The law will be attractive to foreign governments (such as the U.K.) because it enables them to enter into executive agreements with the U.S. which would then allow them to submit requests for electronic data directly to U.S. companies. The law reforms the current mutual legal assistance process in that requests for electronic data will be made pursuant to the requesting countries' laws, and because the requests can be made directly to the providers it bypasses a slow U.S. court system. The law expands upon earlier iterations of similar proposals regarding cross-border data and sets standards that countries have to meet before qualifying for an agreement. It also establishes the boundaries for what the requests can include.[83]

In addition to amending the SCA, the CLOUD Act also amends parts of ECPA and the Wiretap Act to allow providers to permit disclosures to foreign governments who entered into these executive agreements. The new law thus provides legal clarity for companies operating overseas, and it will dramatically minimize the conflict of law issues that had been a source of enormous frustration for both private industry and foreign governments for several years now.

---

81. Morgan Chalfant, *U.S., British Officials Push Deal on Cross-Border Data Access for Law Enforcement*, THE HILL (June 15, 2017), http://thehill.com/policy/cybersecurity/337997-us-british-officials-push-deal-to-improve-law-enforcement-access-to-data.

82. The CLOUD Act, S. 2383, 115th Cong. (2018) (emphasis added), https://www.hatch.senate.gov/ public/_cache/files/6ba62ebd-52ca-4cf8-9bd0-818a953448f7/ALB18102%20(1).pdf.

83. *See* TIFFANY LIN & MAILYN FIDLER, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y AT HARV. U, at 4 (Sept. 2017); *see also* DOJ's earlier proposal for cross-border data access reform, https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p4.

There has been a push for an agreement for this type of legal framework since the end of the Obama administration.[84] The hope is that an agreement of this kind will pave the way for future agreements with other qualifying countries. Proponents of the CLOUD Act also hope it will forestall some of the more damaging alternative responses foreign governments are considering in response to current U.S. law on data access. To re-iterate, these responses could include expanding surveillance capabilities, limiting use of encryption, mandating data localization, expanding extraterritorial application of laws, letting private companies "hack back" against hostile cyber activity and/or letting law enforcement build backdoors into systems.[85] All of these things are adverse to U.S. interests.

A. *Important Protections Included in the New Legislation*

The CLOUD Act is an improvement upon many earlier proposals to address the cross-border data problem. It leaves intact the main framework of an earlier proposal by the Department of Justice which called for executive agreements of this type.[86] Privacy and civil liberties advocates may not be totally satisfied with the CLOUD Act's provisions, but the new law actually addresses privacy concerns much more comprehensively than they might acknowledge at first glance, and their earlier criticisms of previous legislative options in this area have been directly addressed in this new legislation.[87]

One of the earlier criticisms was that the executive agreements concentrate too much power in one branch of government.[88] The concern was that the vetting of countries was going to be done solely by the executive, which raised separation of power questions, and heightened the anxiety that the executive branch could honor a dubious legal assistance request or enter into an agreement without any Congressional input. The CLOUD Act provides that the executive agreements only go into force after notice to Congress and a 180-day waiting period. A joint resolution of disapproval issued during those 180 days will nullify the agreement. There is also a requirement for a new review if the

84. Alan Travis, *Secret Report Urges Treaty Forcing U.S. Web Firms' Cooperation in data Sharing*, THE GUARDIAN (June 2, 2015), https://www.theguardian.com/world/2015/jun/02/web-firms-data-sharing-secret-treaty.

85. *See* Lin & Fidler, *supra* note 83, at 4.

86. U.S. DEP'T OF JUSTICE, *supra* note 6.

87. *See e.g.*, CTR. FOR DEMOCRACY & TECH., CROSS-BORDER LAW ENFORCEMENT DEMANDS: ANALYSIS OF THE US DEPARTMENT OF JUSTICE'S PROPOSED BILL (Aug. 17, 2016), https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf; AM. CIVIL LIBERTIES UNION, AMNESTY INT'L & HUMAN RIGHTS WATCH, RE: DEPARTMENT OF JUSTICE PROPOSAL ON CROSS BORDER DATA SHARING, AMENDING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AND THE WIRETAP ACT (Aug. 9, 2016), https://www.aclu.org/sites/default/files/field_document/letter_to_hill_re_doj_mlat_reform_proposal_final.pdf.

88. *See* Robyn Greene, *The Cloud Act Still Poses a Threat to Privacy and Human Rights*, JUST SECURITY (Mar. 23, 2018), https://www.justsecurity.org/54242/improved-cloud-act-poses-threat-privacy-human-rights.

underlying bilateral executive agreements change. Thus, this new language provides an avenue for the legislative branch to weigh in and when appropriate, provide an important check on executive power.

Second, the law addresses earlier criticisms about the legal standards of foreign countries and provides that the executive agreements between nations have to meet a stringent set of requirements. Andrew Keane Woods, a professor of law at the University of Kentucky, and Peter Swire of Georgia Tech, both experts on cross-border data access reform, note that the bill specifies that the Attorney General, with the concurrence of the Secretary of State, must determine that the foreign government meets three essential stipulations:

> (1) The country has "robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement" (the robustness of these protections are to be determined by a checklist of human rights and other rule of law standards).
> (2) The foreign government has adopted minimization procedures regarding information concerning US persons; and
> (3) The agreement has protections to prevent the foreign government from targeting or collecting information about US persons or persons located in the US, and to prevent the US government from requesting the foreign government to use the agreement as a runaround on current restrictions on data collection.[89]

The thrust of this language ensures that the countries with which the United States engages in data transfers are committed to the rule of law, and have a process in place to appropriately govern this arrangement. It is an important safeguard against the potential to enter into agreements with countries that do not meet our legal standards, and it also forces other countries who may want to enter into such agreements with the U.S. to improve their own legal foundations. Over time, it could incentivize other countries to adopt legal positions that raise privacy protections.[90]

Further, requests from the foreign government must be lawful, meaning they must comply with the foreign government's domestic law. Critics have argued that the language of the bill does not actually require judicial review,[91] but this criticism is misplaced as the text explicitly says that the request (v.) "shall be subject to review or oversight by a court, judge, magistrate or other independent authority prior to, or in proceedings regarding, enforcement of the

89. Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018, 5:49 PM), https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

90. *See* Jennifer Daskal, *New Bill Would Moot Microsoft Ireland Case — And Much More!*, JUST SECURITY (Feb. 6, 2018), https://www.justsecurity.org/51886/bill-moot-microsoft-ireland-case-more.

91. *See* Sharon Bradford Franklin, *Left Out of the Party on Cloud Nine: A Response to Jennifer Daskal*, JUST SECURITY (Feb. 13, 2018), https://www.justsecurity.org/52189/left-party-cloud-nine.

order."[92] The language was strengthened from previous versions of the law to ensure the oversight of a judge or independent authority happens "prior to" the request being made and approved. Critics argue that the addition of the words "or in proceedings regarding" effectively means that "prior to" is not a requirement. However, this criticism is also misplaced. The addition of this language should still be read as a mandate for judicial involvement.[93] The addition of the words "or in proceedings regarding" and "oversight *or* review" is effectively an acknowledgement that other countries have legal systems that are different from our own.[94] Experts Jennifer Daskal and Peter Swire, who have worked this issue in conjunction with privacy advocates, explained previously that "while independent judicial review is an imperative requirement of the U.S. legal system, France and many other civil law countries have a criminal justice system in which the judge presiding over a case plays an investigatory role as well. In those nations, there quite possibly is no independent judicial official with jurisdiction separate from the investigating magistrate. If the bill's criteria are too U.S.-centric in requiring review by a fully independent magistrate, many countries with strong rule-of-law traditions and institutions will be unable to participate in any of the agreements envisioned by the CLOUD Act."[95]

Thus, critics miss the important nuance in this language. The text requires judicial involvement by the requesting country, and this should satisfy the concerns from many earlier proposals on this issue. While in some cases this may require "review," it may require "oversight" in others. The point is that a Court in the requesting country must have a say in how data requests operate. It also keeps the door open for other countries to enter into these executive agreements who may not have legal systems that are carbon copies of our own, but are still sufficiently robust.[96]

Further, the CLOUD Act requires compliance reviews after an executive agreement has been entered into and data is flowing. The U.S. Department of Justice is likely to play a key role in these compliance reviews, and it is *possible* that other groups like the ACLU or other privacy advocates may be involved too. These compliance reviews can further ensure that foreign countries' requests for data meet the stringent requirements of the text of the CLOUD Act and that such countries actually meet the requisite standards to be

92. *See* The Cloud Act § 2523 (b)(4)(D)(v).

93. *Id.*

94. *Id.* (emphasis added).

95. Jennifer Daskal & Peter Swire, *Privacy and Civil Liberties Under the CLOUD Act: A Response*, JUST SECURITY (Mar. 21, 2018), https://www.justsecurity.org/54163/privacy-civil-liberties-cloud-act-response.

96. At the time of this paper's publication, it has been reported that the US and the EU are likely to address law enforcement access to data and a potential executive agreement similar to what is being negotiated with the U.K. *See* Jennifer Daskal and Peter Swire, *A Possible US-EU Agreement of Law Enforcement Access to Data*, JUST SECURITY (May 21, 2018), https://www.justsecurity.org/56527/eu-agreement-law-enforcement-access-data.

eligible for executive agreements in the first place. They can therefore help ensure a successful implementation of the CLOUD Act and may also offer an opportunity for grievances to be addressed, and for privacy concerns to be ameliorated if a rigorous enforcement regime is in place. There are calls for these reviews and the executive agreements themselves be made public, and it is possible this may yet be another safeguard.

The law also includes a new mechanism that allows providers to apply for a motion to quash or modify legal process if the provider reasonably believes that the subscriber is not a U.S. person, and that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.[97] A comity provision in the law specifies that a court should conduct an analysis of the interests of the foreign government in the event of such a motion to quash.[98] This language is another improvement that provides further assurance to both private companies and foreign governments that their interests are protected.

The CLOUD Act also now includes important language that directly addresses the issue of "backdoor" requirements for private companies. In a nod to privacy advocates, the text specifies that executive agreements cannot create an obligation for a company to be capable of decrypting data in response to a surveillance request. This further ensures a proper balance of law enforcement and privacy concerns, and directly prohibits one of the more damaging alternative responses foreign governments had been considering in response to previous U.S. law on data access.

Absent a requirement that all foreign countries requesting data have to duplicate U.S. legal standards, it may not have been possible to completely satisfy all civil liberties and privacy advocates with this legislation. However, the CLOUD Act's framework should be embraced by law enforcement and privacy advocates alike. Its basic foundation is a compelling solution to a legal obstacle that was long overdue for a restructuring. The alternative, a legal Catch-22 where foreign governments force providers to store data locally in order to comply with local demands, regardless of U.S. law, is one that privacy advocates cannot possibly argue is a better outcome.[99]

VI. WHY CROSS-BORDER DATA ACCESS REFORM IS A BETTER LEGISLATIVE OPTION TO ADDRESS CYBER THREATS THAN ACDC

Changing the rules for cross-border data access will be far from the silver bullet that stops cyber actors from hacking American industry, but it is a less risky way to address the cyber threat, and it can avoid some of the problems

97. *See* Woods & Swire, *supra* note 89.

98. Consolidated Appropriations Act § 2713(h)(2) (2018).

99. *See* Stephen Dockery, *Data Localization Takes Off as Regulation Uncertainty Continues*, WALL ST. J.: BLOG (June 6, 2016), https://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues.

that ACDC presents. In particular, reforming the cross-border data access process can actually assist with cyber attribution in ways that do not raise the thorny issues that ACDC does. For example, with the CLOUD Act's provisions in place, a U.S. company that is the victim of a cyber-intrusion emanating from a foreign network can go to the FBI for assistance, who can then go directly to an electronic communications provider in that country where the intrusion was facilitated, and request electronic data related to that intrusion. Under the new rules, so long as there is an executive agreement in place with the country where the intrusion originated, the FBI would not have to rely on meeting the foreign country's legal standards, and the process itself would be exponentially faster. Where ACDC would involve the presumably unauthorized access of foreign private networks to gather data about cyber intrusions, the CLOUD Act seeks an agreed upon bilateral solution, and the attribution investigation would be conducted by a competent law enforcement agency in coordination with a service provider who has the affirmative authority to gather such information.

To be sure, cyber attribution investigations today can rely on the consent of foreign network owners whose infrastructure may have been unwittingly co-opted by attackers, and countries can still engage in joint investigations or work through other mechanisms, but the update in the law clarifies for providers and owners of infrastructure what their obligations are. The previous issues with conflicts of law that burdened private companies operating overseas would be dramatically minimized so long as an agreement were in place between the countries where such a company is operating. The CLOUD Act will certainly not solve the attribution problem, and it may not even get the same type of data that a sophisticated defender using active cyber defense countermeasures could get, but it can still help identify nefarious activity.

The University of Kentucky's Andrew Keane Woods has suggested that it is likely that Robert Mueller's team learned the names of individual Russians and their roles within the conspiracy to hack the American election of 2016 through use of the SCA, and potentially, access to data across borders.[100] Basing his analysis on the unsealed indictment of the Russian hackers, Woods explains that because the individual Russians were operating overseas, it is likely that their computer data passed through servers in Europe in addition to the U.S., and though we cannot know for sure, it is likely that Mueller's team operated under the SCA to compel U.S. service providers, like Twitter, Google and Facebook, to produce the suspects' accounts.[101] Woods concludes that even if Mueller's team only accessed U.S. held evidence, it is clear that the problem of election interference, and computer hacking emanating from overseas is not going away, and that Mueller's indictments provide the U.S. with "powerful circumstantial evidence that access to data across borders is

100. *See* Andrew Keane Woods, *Mueller's Indictment of Russian Hackers Highlights the Stakes of the Microsoft Case*, LAWFARE (Feb. 17, 2018, 1:27 PM), https://www.lawfareblog.com/muellers-indictment-russian-hackers-highlights-stakes-microsoft-case.

101. *Id.*

critical for solving not just crimes, but perhaps some of the most consequential crimes of our era."[102]

Perhaps most importantly, the CLOUD Act helps establish the international norm in cross-border investigations that "hacking back" (absent some sort of comparable cyber treaty that would authorize such activity) would undermine. Cross-border data access reform could therefore be a building block towards better international cooperation on cyber. Even if the U.S. is unlikely to get an agreement in place with countries where the most serious and sophisticated intrusions are coming from, agreements with allied countries can still be a positive step forward in setting an international standard.[103] Because cyber treaties may be difficult to come by with adversaries, much less be verifiable, an agreement between partners may be the best place to start.[104] Moreover, since many cyber intrusions today involve the co-opting of infrastructure outside of the original source of the attack, agreements between allied nations that facilitate cross-border data investigations where such infrastructure has been so co-opted may go further than one might assume.[105]

Active cyber defense implicates some very controversial areas of foreign policy and international law. Enacting ACDC into law before an international consensus is built about what is and what is not acceptable in this area is fraught with danger. The United States risks serious retaliation from countries where we have "hacked back." However, once an agreement is in place for how data may be accessed between like-minded countries, other agreements could follow.

For instance, if a consensus could be built around how to access data across borders, and about when certain laws apply or do not apply extraterritorially, it could build towards a discussion about what data access tactics fit outside the SCA and may not require a formal legal assistance request at all. To illustrate, the updated draft of ACDC includes a carve-out for "attributional technology" (defined as programs/codes or commands that beacons or returns locational or attributional data in response to a cyber-intrusion) and distinguishes such technology from "active cyber defense" altogether. This type of technology is generally seen as less controversial if implemented properly and with common understanding about how it works. Depending on how "attributional technology" actually operates and what other countries are inclined to allow, it might eventually fit into a category outside of the legal assistance process.

In the interim, while attributional technology continues to evolve (alongside the legal complexities) the best thing the private sector can be doing to harden their own networks against hostile cyber actors, is to simply practice good network hygiene. Most practitioners suggest that traditional security

---

102. *Id.*

103. *See* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View,* HOOVER INSTITUTION, STANFORD UNIVERSITY (Mar. 9, 2011).

104. *Id.*

105. *Id.*

measures are often effective against the more common threat actors.[106] Thus, routine application of cyber patches, software updates, anti-virus software etc. is going to go a long way in thwarting most hostile cyber activity. For particularly sophisticated or advanced threat actors, the way forward will likely be rooted in information sharing among victims. While the framework for an information sharing program among victims also continues to evolve, many experts agree that this is the foundation for a robust cyber defense program.[107]

Smart legislation, however, can still help in this fight. The CLOUD Act is a positive step forward that updates a legal framework that was not optimized for today's technological challenges and cyber threat environment. Without any changes to the previous legal system, other countries did not have incentive to reform their own laws to access U.S. held data, and could have been expected to mount efforts to get the data via surreptitious tactics[108] (up to and potentially including "hack back" authority). These developments would obviously not serve the interests of either privacy advocates or U.S. policy goals. Congress was wise to embrace the calls for change. The next step will be to ensure the successful implementation of the CLOUD Act itself and the forthcoming executive agreements that the CLOUD Act sets the parameters for. As the U.S. government considers, negotiates, and enters into these executive agreements, the goal should now be to ensure that the agreements meet the objectives/values/principles that the legislation is intended to uphold.

CONCLUSION

The onslaught of cyber-attacks is rightly causing a re-examination of what can be done to combat the threat. However, legalizing "hack-back" by private entities is fraught with extremely difficult legal and foreign policy complexities. Even other defense measures short of "hacking back" are problematic if they involve going onto outside networks without consent of foreign network owners or by relevant foreign authorities. The embedded risks for escalation, deterioration of the United States' efforts to establish international rules, misattribution, and the breaking down of current cyber norms may prove to be too much of a hurdle for the current legislative proposal to overcome. It is understandable why many are calling for the deployment of active cyber defense methods, but the real question is what price would we pay for this capability? Admiral Mike Rogers, the former Director of the National

106. *See* CSIS/DOJ ACTIVE CYBER DEFENSE EXPERTS ROUNDTABLE (Mar. 10, 2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf

107. Andrew Tannenbaum, *To Prevent Cyberattacks, Share the Threat Data*, WALL ST. J. (July 9, 2015), https://www.wsj.com/articles/to-prevent-cyberattacks-share-the-threat-data-1436482349.

108. *See* Jennifer Daskal & Andrew Keane Woods, *Congress Should Embrace the DoJ's Cross-Border Data Fix*, LAWFARE (Aug. 1, 2016, 8:52 AM), https://www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0.

Security Agency, expressed to the House Armed Services Committee that hacking back "puts more gunfighters out on the street in the Wild West."[109] He is not alone among the national security establishment who hold this sentiment.

Congress may be able to reassess language in the Computer Fraud and Abuse Act that constrains some activity as it relates to active defense, but any activity where cyber effects are felt on an outside network are going to be problematic. Thus, Congress needs to consider additional measures to address attacks from outside networks. If Congress moves forward on ACDC, it should first clear up the significant amount of definitional ambiguity in the current bill, and be prepared to be extremely conservative with the particulars about what it authorizes. The government should also be prepared to pull back on overly-aggressive active cyber defense measures when necessary.

The creation of norms in cyberspace is going to be more difficult than giving companies and individuals the ability to exact retribution, but absent an international framework for regulation of active cyber defense, it is quite possible that allowing "hacking back" would be make an already dangerous problem even worse and more complicated. The international community has made a number of significant advances in building consensus on what laws, rules, and norms are applicable in cyberspace, but there is scarce international law on active cyber defense in particular. Enacting the ACDC without building an international consensus on these issues is very risky. We can expect foreign nations, even allied ones, to retaliate against us.

Alternatively, cross-border data access reform is an area where Congress has enacted meaningful legislation as it relates to international norms. The previous system for cross-border investigations involving electronic communications and other digital evidence was broken as the Stored Communications Act had not been amended to address the transforming legal and technological landscape. The CLOUD Act will not by itself solve all cross-border data issues, but it forms the basis for a very promising solution, and its basic framework paves the way for the U.S. to address the issue with allied nations. Once agreements between countries are in place, it should streamline international cyber (and other criminal) investigations, and it should also incentivize other countries to reform their own legal processes in order to be included in future or proposed executive agreements.[110]

Cross-border data access reform could also help with the attribution problem by assisting cyber investigations where computer data is held overseas. With the CLOUD Act and executive agreements in place, American companies would not have to worry about conflicting laws of other countries, and the overall speed of the process would be increased immensely. American law enforcement will also get reciprocal rights in other countries. While cross-border data access reform would not necessarily get better data on cyber

109. Sean D. Carberry May, *Congressman Files New 'Hack Back' Bill*, *FCW* (May 26, 2017), https://fcw.com/articles/2017/05/26/graves-hack-back-bill.aspx.

110. *See* Daskal & Woods, *supra* note 108.

intrusions than active cyber defense measures could, it will however, establish an international solution via bilateral agreements. The ACDC, by contrast, would be a direct challenge to the international norms the U.S. has been working towards for years. The ancillary benefit of reform could also pave the way and set the standard for future cooperation on cyber issues among different countries. Beacon technology, or locational/attributional data, as mentioned, is one carve-out in the ACDC proposal where there might be room for international cooperation, but it certainly would not hurt to have bilateral agreements in place for cross border data investigations to help move this discussion forward.

The forthcoming executive agreements between countries and the process by which these executive agreements are entered into along with the compliance reviews that the CLOUD Act specifies offer another safeguarding mechanism that should ensure a robust oversight construct. It is possible that privacy groups and other potential skeptics of this new legal framework will have a role to play in this process, but to the extent that the new law does not satisfy every single one of their concerns, the implementation phase of the executive agreements provide yet another opportunity to ensure the law works the way it is intended and in the best way possible for all parties. Privacy advocates and others should therefore embrace the new framework and focus now on how to certify its successful application.

Cross-border data access reform is not a panacea. There are several other policy options and tools out there in this fight. Where current proposed legislation is concerned, however, the CLOUD Act is a step in the right direction that better harmonizes and updates the international law enforcement framework to meet today's technological challenges in a way that ACDC does not. Over time, as attribution technology improves, cross-border data investigations and their facilitation through bilateral agreements like the one proposed by the CLOUD Act, could function as a strong component of strategic cyber deterrence. If nefarious actors know that they cannot easily co-opt the infrastructure of third party countries where the U.S. has strong executive agreements for data access in place, it reduces the avenues through which hostile cyber actors can operate. It could also be a tool to help narrow down the true source of cyber intrusions.

Cross-border data access reform, if implemented properly, can be a much less controversial way for Congress to help combat cybersecurity challenges than the ACDC. Without an updated framework in place, or without an agreement with our allies (at the least) about what can be done together to combat this threat, the cyber domain will remain vulnerable, bad actors will continue to exploit the legal weaknesses in our system, and the asymmetric power balance against the U.S. will continue to grow. We are not powerless against these threats, but we should act wisely before making them worse.