NOTES

WHO DECIDES? SPEECH AND PRIVACY RISKS IN THE DRAFT SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION

COURTNEY CHRISTENSEN*

ABSTRACT

Currently, in order to solve crimes that occur domestically but for which evidence is in a foreign country, law enforcement authorities of one country outreach to the evidence-storing country through procedures set in Mutual Legal Assistance (MLA) treaties. The MLA process is most frequently used to access electronic data gathered by internet service providers located in another country. However, current MLA processes are slow and often ineffective; therefore, a second optional protocol is being proposed to the Budapest Convention, which currently dictates MLA procedures, to streamline the process. This Note argues that the United States should reject this proposed protocol as the changes, which would allow law enforcement to make direct demands on internet service providers and minimize the information presented about crimes to those providers, would threaten speech and privacy laws and ideals of the United States.

---

* J.D. 2021. Special thanks to Professors Stewart and Regan for their continued assistance and support in the drafting of this Note. All mistakes herein are my own. This Note was drafted in 2021, before recent developments including the adoption of the Second Additional Protocol to the Budapest Convention by the Committee of Ministers of the Council of Europe. The text of the Protocol should be opened for signatures in May 2022. S*ee Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe*, COUNCIL OF EUR. (Nov. 17, 2021), https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe.

I. INTRODUCTION

Imagine that an individual in Germany posts a message online insisting that the Holocaust never occurred. The online post receives large public attention, including the attention of local law enforcement. In Germany, posting publicly about Holocaust denial is a crime punishable by up to five years in prison,[1] and German authorities want to prosecute the author of the post. However, the investigation stalls because the individual posted the message anonymously. Nonetheless, the German authorities know they can likely discover this individual's identity by tracking the individual's IP address. Finding the IP address presents a further issue, however, as the internet service provider that has access to the individual's IP address is located in the United States. Therefore, the German law enforcement officers now need to collect electronic evidence stored in the United States through a process that will allow the evidence to be admissible in German courts—how will this be done?

Mutual Legal Assistance (MLA) treaties were designed to solve this very problem. MLA treaties allow foreign governments to access evidence of crimes stored in another country through an admissible and, hopefully, expedient process.[2] To utilize the current MLA system, the investigating law enforcement agency in one country files a request for the evidence through a specialized domestic "central authority" in the country in which the sought-after evidence is stored; in the United States, the "central authority" is the Department of Justice's Office of International Affairs.[3] If the Department of Justice approves the

1. Strafgesetzbuch [StGB] [Penal Code] § 130(3) (Ger.), https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html; Dylan Fotiadis, *Undeniably Difficult: Extradition and Genocide Denial Laws*, 17 WASH. U. GLOB. STUD. L. REV. 677, 686 (2018).

2. CYBERCRIME CONVENTION COMM., COUNCIL OF EUR., CRIMINAL JUSTICE ACCESS TO DATA IN THE CLOUD: CHALLENGES 15 (May 2015), https://rm.coe.int/1680304b59 [hereinafter Criminal Justice Access: Challenges].

3. CYBERCRIME CONVENTION COMM., COUNCIL OF EUR., T-CY ASSESSMENT REPORT: THE MUTUAL LEGAL ASSISTANCE PROVISIONS OF THE BUDAPEST CONVENTION ON CYBERCRIME 99 (Dec. 2014), https://rm.coe.int/16802e726c [hereinafter Assessment Report]; Christine Galvanga, *The*

evidentiary request by assuring that certain conditions are met, the request is then sent to the appropriate U.S. Attorney's Office, which will present the evidence request to a federal magistrate.[4] The federal magistrate will ensure the request complies with U.S. law and the U.S. Constitution and then issue a U.S. warrant to the relevant company for the requested evidence.[5] The company then sends the requested evidence to the Department of Justice, which, after reviewing the evidence to ensure that certain minimization and human rights requirements are met, sends the information back to the requesting government's "central authority," which passes the information onto the investigating law enforcement agency.[6]

However, the current MLA process can be prohibitively time intensive and too complex to be useful.[7] Requests can take anywhere from six to twenty-four months to process in the United States,[8] and investigations are often abandoned due to MLA complications.[9] Foreign law enforcement officers are particularly frustrated with the United States, where many of the world's internet service providers are located and much of the world's data is stored.[10]

Returning to the posed hypothetical, an evidentiary request from Germany to the United States about the crime of Holocaust denial would likely be denied by either the Department of Justice or the federal magistrate reviewing the request, as the request would not comply with U.S. law and constitutional requirements.[11] In the United States,

---

Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform, 9 NOTRE DAME J. INT'L COMP. L. 57, 60 (2019).

4. STEPHEN P. MULLIGAN, CONG. RSCH. SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT (2018).

5. *Id.*; Assessment Report, *supra* note 4, at 37; Galvanga, *supra* note 4, at 60.

6. Galvanga, *supra* note 4, at 60.

7. CYBERCRIME CONVENTION COMM., COUNCIL OF EUR., CRIMINAL JUSTICE ACCESS TO DATA IN THE CLOUD: RECOMMENDATIONS 9 (Sept. 2016), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

8. *Id.*

9. *Id.*

10. CYBERCRIME CONVENTION COMM., COUNCIL OF EUR., CRIMINAL JUSTICE ACCESS TO DATA IN THE CLOUD: COOPERATION WITH "FOREIGN" SERVICE PROVIDERS 4 (May 2016), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d.

11. Under the current MLA process, courts review evidentiary requests to ensure that it complies with the underlying treaty, U.S. law, and the U.S. Constitution. MULLIGAN, *supra* note 5, at 14.

the First Amendment provides broad protection of speech, even if the speech is hateful and/or derogatory.[12]

A proposed second additional protocol to the Budapest Convention on Cybercrime, a 2001 treaty designed to more effectively combat cybercrime,[13] which the United States is party to, could drastically change the result of the MLA process.[14] A working group created by the original Budapest Convention prepared a draft second additional protocol to improve the current issues in the MLA process.[15] One provision in the proposed protocol would allow foreign law enforcement officers to make a "direct demand" on a U.S. internet service provider for a subscriber's data without going through the Department of Justice's Office of International Affairs.[16] As stated in section 4.1 of the proposed protocol,

> each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, to obtain disclosure of specified, stored subscriber information in that service provider's possession or control, where the information is needed for the issuing Party's specific criminal investigations or proceedings.[17]

The proposed provision will go beyond Article 18.3 of the original Budapest Convention, the first attempt to create a process by which governments can gain information from internet service providers,[18] as

12. *See, e.g.*, Snyder v. Phelps, 562 U.S. 443, 461 (2011) (holding that speech which constituted intentional infliction of emotional distress was protected by the First Amendment); R.A.V. v. City of Saint Paul, 505 U.S. 377, 393 (1992).

13. *See* Convention on Cybercrime, Preamble, Nov. 23, 2001, E.T.S. No. 185 [hereinafter Budapest Convention].

14. *See Joint Civil Society Response to the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime*, COUNCIL OF EUR. 1, 3 (Nov. 7, 2019), https://rm.coe.int/civilsocietysubmission-t-cydraftsecondadditionalprotocol/168098bc6d [hereinafter Joint Civil Society Response].

15. *See* CYBERCRIME CONVENTION COMM., COUNCIL OF EUR., ENHANCED INTERNATIONAL COOPERATION ON CYBERCRIME AND ELECTRONIC EVIDENCE: TOWARDS A PROTOCOL TO THE BUDAPEST CONVENTION 2 (Sept. 5, 2019), https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07 [hereinafter Enhanced International Cooperation].

16. CYBERCRIME CONVENTION COMM., COUNCIL OF EUR., PREPARATION OF A 2ND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION ON CYBERCRIME 15 (2018), https://rm.coe.int/provisional-text-of-provisions-2nd-protocol/168098c93c [hereinafter Draft Provisions].

17. *Id.*

18. Budapest Convention, *supra* note 14, art. 18.

parties will now be able to issue orders to providers in another party's territory.[19]

The proposed protocol further includes other provisions that enhance the MLA process. For example, the proposed protocol does not include a dual criminality requirement; dual criminality is the legal principle that the offence prosecuted in one state also constitutes a crime in the state in which the evidence is being requested.[20] The proposed protocol also does not require that the requesting party supply a summary of the facts regarding the investigation.[21] Finally, the proposed text requires party states to create implementing legislation to ensure that internet service providers "give effect" to the requests for evidence by shielding the internet service providers from liability for complying with evidentiary requests under the protocol and by creating an enforcement mechanism if the internet service companies do not comply with these requests.[22] The proposed language provides discretion to parties regarding enforcement mechanisms but suggests that parties enforce foreign law enforcement evidentiary demands as they would enforce domestic warrants.[23] These changes represent a "drastic expansion of cross-border data access powers."[24]

Returning to the original hypothetical regarding Germany's investigation into an online post about Holocaust denial, the proposed changes in the additional protocol would create a different outcome. Germany, which is a party to the Budapest Convention, would now reach out directly to the U.S. internet service provider that has access to the suspect's information instead of the Department of Justice's Office of International Affairs. The internet service provider might well comply with the request, given the threat of some form of enforcement action for non-compliance, and provide the individual's information to the German law enforcement authorities. Not only will the evidence

19. "Specifically, that Article [18] applies when a service provider is 'in the territory' of the issuing Party (see Article 18.1.a of the Convention) or 'offering its services' in the issuing Party (see Article 18.1.b). Given the limits of Article 18 and the challenges facing mutual assistance, it was considered important to establish a complementary mechanism that would enable more effective cross-border access to information needed for criminal investigations and proceedings. Accordingly, the scope of this Article goes beyond the scope of Article 18 of the Convention by allowing a Party to issue certain orders to service providers in the territory of another Party." Draft Provisions, *supra* note 17, §§ 2.2, 4.2(5).

20. Joint Civil Society Response, *supra* note 15, at 3.

21. Draft Provisions, *supra* note 17, § 4.1(3)-(4).

22. *Id.* §§ 4.2(7), 5.2(6).

23. *Id.*

24. Joint Civil Society Response, *supra* note 15, at 3.

collection process be much faster, but the German authorities will receive the evidence they are requesting. German authorities now have an improved chance of completing the full extent of their investigation into Holocaust denial and prosecuting the individual who authored the online post.

However, in the United States, the new result achieved under the changes proposed by the protocol will implicate the freedom of speech protected by the First Amendment, which would likely protect posts that deny the Holocaust.[25] Additionally, the proposed changes to the MLA process may implicate privacy rights as law enforcement officers will be making evidentiary demands directly on internet service providers without domestic judicial review or an appeals process.

While countries are generally presumed to have jurisdiction over individuals who commit a crime in their territory, speech, and particularly online speech, poses a different type of potential crime. Online speech occurs not only in the country in which the author posts the speech; the author's conduct also occurs in countries, such as the United States. The United States retains an interest in protecting speech that occurs in its borders. An elimination of the dual criminality requirement would allow the law enforcement of one state to penalize and thereby chill speech worldwide. [26]

Given the difference of laws among parties to the convention relating to speech and privacy protection, the proposed protocol shifts too much power to foreign law enforcement agencies and the private sector to make determinations about speech and privacy rights. The problematic shift in power is demonstrated by examining the two most likely responses that internet service providers might have to a direct demand for subscribers' information from a foreign law enforcement agency: complete and automatic compliance with every request or compliance with requests on a case-by-case basis.

Each option represents a different danger to both speech and privacy. Complying with every request would allow foreign law enforcement agencies to make determinations regarding speech and privacy rights, while complying with requests on a piecemeal basis would allow private companies to make these determinations on speech and privacy. Overall, the very idea that internet service providers can choose which approach to take creates the danger of companies choosing which actors decide the boundaries of speech and privacy rights.

25. U.S. CONST. amend. I; Snyder v. Phelps, 562 U.S. 443, 461 (2011).

26. Many thanks to professor Mitt Regan for help formulating this idea.

II. Compliance with Every Request

If the protocol is enacted as currently drafted, some internet service providers will likely comply with every request for a subscribers' data, allowing foreign governments to dictate which acts deserve to be investigated as a crime, and which crimes warrant an invasion of privacy. The protocol's structure, which provides liability protection for companies that comply with requests and punishment for companies that do not comply with requests, is an example of a government exerting effective control over a private company through a "combination of carrots and sticks."[27] Companies who are attempting to avoid conflict, reduce legal uncertainty, and maintain a stable relationship with governments will have a large incentive to comply with these requests.[28] Smaller- and medium-sized internet service providers will likely be more susceptible to this control, as they are unlikely to have access to the legal or human resources that would allow them to fight these requests or endure the potential punishment for non-compliance. This section will address how an internet service provider's compliance with every evidentiary request under the proposed protocol allows foreign governments to establish global standards for appropriate speech and privacy protections through their law enforcement agencies.

A. *Threat of a Chilling Effect on Speech*

As many parties to the Budapest Convention criminalize speech that would be protected in the United States, complying with all requests for evidence would place companies in a position in which they are assisting investigations and prosecutions for acts that are legal in the United States. This will create a chilling effect on speech.

1. Explanation of the Chilling Effect

A chilling effect on speech occurs when a government action indirectly deters an individual from speaking.[29] In the context of the United States, "a chilling effect occurs when individuals seeking to engage in activity protected by the First Amendment are deterred from so doing by governmental regulation not specifically directed at the

27. Jack M. Balkin, *Old School/New-School Speech Regulation*, 127 Harv. L. Rev. 2296, 2298–99 (2014).

28. *Id.*

29. Monica Youn, *The Chilling Effect and The Problem of Private Action*, 66 Vand. L. Rev. 1473, 1474 (2013).

protected activity."[30] As a chilling effect stems from a fear of *any* future consequences, it is not limited to government action; a chilling effect also extends to private reactions that are enabled by the government.[31]

The proposed changes to the Budapest Convention, particularly the lack of a dual criminality requirement, create just the type of government-enabled private reactions that would result in a chilling effect. In their response to the proposed protocol, the Center for Democracy and Technology explained,

> the [second additional] protocol permits a country that, for example, makes blasphemy a crime, to issue an order for disclosure of subscriber information to prosecute that crime to a service provider in a country in which the blasphemy is protected free expression. This puts the free expression rights of people around the world at risk if they use a service provider with a global user base.[32]

The direct demand for evidence for the crime of blasphemy provides a very real example to the ACLU's concern that the lack of a dual criminality component allows one country to dictate removal of certain items on the internet across the world, regardless of whether the post would be criminal within an individual party's jurisdiction.[33]

Although the internet service provider will not be taking down potentially lawful online speech directly, the providers will be releasing information to a government law enforcement agency that could lead directly to the speaker's identity and whereabouts. Once the government has this information, the speaker could be arrested and/or otherwise forced to remove the content themselves. This process will result in the removal of speech that is otherwise protected in the United States from the internet across the world via the aid of a private U.S. company.

The chilling effect will be especially important with regard to anonymous speech. As stated by the Joint Civil Society Response to the draft provisions,

---

30. *Id.* at 1482.

31. *Id.* at 1475.

32. Ctr. for Democracy and Tech., *Initial Observations of the Center for Democracy* & Technology on the Provisional Draft Text of the Second Additional Protocol to the Budapest Convention on Cybercrime, COUNCIL OF EUR. *1, 5* (2019), https://rm.coe.int/cdt-comments-2nd-additional-protocol/168098c93e [hereinafter CDT comments].

33. *Seven Reasons the US Should Reject the International Cybercrime Treaty*, ACLU, https://www.aclu.org/other/seven-reasons-us-should-reject-international-cybercrime-treaty (last visited Apr. 18, 2020).

> legal safeguards . . . are vital because fear of reprisal might chill critical discussions of public matters of importance. [Fear of reprisal] will also chill [people's] freedom to form their thoughts and opinions in private, free from intrusive oversight by governmental entities. Any online subscriber who does not want his or her speech connected to their permanent identity has an interest in anonymity. Online speakers may be concerned about political or economic retribution, harassment, or even threats to their lives.[34]

By allowing foreign governments to demand information from internet service providers that would allow them to identify anonymous critics or journalist, the proposed protocol would not only result in the punishment for speech that is not a crime, but would also deter these actors, who can be vital to exposing government corruption or abuse, from even speaking in the first place.

2. Likelihood of a Resulting Chilling Effect

If the proposed protocol is enacted as currently drafted, a chilling effect will likely occur due to the requirement that ratifying parties create some type of legal consequence for companies that fail to comply with direct orders from foreign law enforcement.[35] The requirement of a consequence for failure to comply creates what Jack Balkin refers to as "collateral censorship." Collateral censorship occurs when:

> the state holds private party A liable for the speech of another private party, B, and A has the power to block, censor[,] or otherwise control access to B's speech . . . This will lead A to block B's speech or withdraw infrastructure support from B. In fact, because A's own speech is not involved, A has incentives to err on the side of caution and restrict even fully protected speech in order to avoid any chance of liability.[36]

For example, social media companies are involved in collateral censorship when they comply with Europe's "right to be forgotten" policy: to avoid financial penalties, companies adopt a default policy in favor

34. Joint Civil Society Response, *supra* note 15, at 9.

35. For example, a party could treat the direct request the same as if it was issued under domestic authority and apply the same consequences. Draft Provisions, *supra* note 17, at §§ 4.2 (7), 5.2(6).

36. Balkin, *supra* note 28, at 2309.

of deletion.[37] The companies will be overly cautious and delete speech that does not qualify for deletion under the "right to be forgotten" policy; thereby chilling lawful speech.[38] Applied in the context of the proposed protocol, internet service providers will be enticed to comply with orders for subscribers' information, even if the subscriber is being investigated for lawful speech. Under the collateral censorship theory, these companies are more likely to protect their own business interests at the expense of sacrificing users' speech rights.

Additionally, evidence shows that the legal framework imagined by the additional protocol actually has the effect of chilling speech, as seen in a study of an analogous framework in the realm of intellectual property. A similar "private enforcement" method is used to fight copyright infringement under section 512 of the Digital Millennium Copy Right Act.[39] In essence, section 512 provides a liability shield for online service providers who implement policies to monitor their users' content for copyrighted material, including the use of "takedown" procedures, or the process by which companies remove a user's content if the content poses a copyright threat.[40] After reviewing the implementation of section 512 by private companies, Professors Jennifer Urban and Laura Quilter found that at least one third of takedown notices given to users, which are messages to users that their speech was removed for copyright reasons, contained a legal flaw and raised "significant" questions about the enforceability in an actual court of law or raised "concerns about the fairness of the process" for selecting which posts to remove.[41] These results show that in approximately one third of cases, companies were removing what may be perfectly legally-protected speech.[42] Given the similarities of the liability shield between section 512 and the second additional protocol, a chilling effect will likely occur should the second additional protocol be implemented as currently drafted.

---

37. Hannah Bloch-Wehba, *Global Platform Governance: Private Power in the Shadow,* 72 SMU L. REV. 27, 58 (2019).

38. *Id.*

39. Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices under Section 215 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUT. & HIGH TECH. L.J. 621, 622 (2006).

40. *Id.*; 17 U.S.C.A. § 512 (West, Westlaw through Pub. L. 117-44).

41. It should be noted that the authors of this study admit that they were examining a small data set and further study is needed to ensure the most accurate results. Urban & Quilter, *supra* note 40, at 622.

42. *See id.*

3. Consequences of the Chilling Effect

Allowing foreign law enforcement agencies to make demands for information on U.S. companies is concerning because these foreign agencies will thereby be controlling which type of speech is deterred or allowed. However, the United States provides greater protection for speech than most other governments that are party to the convention. The difference in speech protection is displayed even within the context of the Budapest Convention. Many parties to the original Budapest Convention are also party to the first additional protocol to the convention, which criminalized racist and xenophobic acts committed through computer systems.[43] Under the first protocol, racist and xenophobic material is defined as:

> any written material, any image[,] or any other representation of ideas or theories, which advocates, promotes[,] or incites hatred, discrimination[,] or violence, against any individual or group of individuals, based on race, color, descent[,] or national or ethnic origin, as well as religion if used as a pretext for any of these factors."[44]

This protocol instructs parties to criminalize behavior such as disseminating racist or xenophobic material online or denying, grossly minimizing, or approving of genocides or crimes against humanity through use of a computer system.[45] However, the United States did not sign the first additional protocol and protects speech such as this under the First Amendment.[46]

Returning to the hypothetical posed in the introduction regarding Holocaust denial, a private company will now have a strong incentive to provide the suspect's information to the German authorities, particularly smaller or medium-sized internet service providers who lack the ability challenge government orders or fight the consequences of noncompliance. Therefore, German authorities will now likely be able to

---

43. Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, *opened for signature* Jan. 28, 2003, E.T.S. No. 189, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

44. *Id.* art. 2.

45. *Id.* art. 3.

46. *Chart of Signatures and Ratifications of Treaty 189*, COUNCIL OF EUR. (2021), https://www.coe.int/en/web/conventions/full-list/?module=signatures-by-treaty&treatynum=189; *see* R.A.V. v. City of Saint Paul, 505 U.S. 377, 393 (1992).

gain access to the user's data from the internet service provider, insist that the user remove the post, and prosecute the individual. These consequences will deter other individuals from posting similar messages and will remove speech that appears legally online in the United States,[47] creating a chilling effect on this type of speech. The process of chilling speech that will occur under the proposed additional protocol allows foreign law enforcement agencies to determine what speech should and should not be allowed on the internet and uses U.S. companies to enact a foreign government's views on the freedom of expression.

B. *Privacy*

Law enforcement will often find it necessary to compromise an individual's privacy—for example, by executing a search warrant—in order to solve a crime. However, in the United States, domestic law enforcement officers do not determine whether an investigation has provided enough evidence to warrant an intrusion into an individual's privacy. Instead, a neutral magistrate determines whether an intrusion is justified during the course of an investigation. If companies comply with every request under the second additional protocol, foreign governments, as opposed to neutral magistrates, will make the final determination regarding the balance between the importance of efficient law enforcement and privacy. As foreign law enforcement agencies will bypass any domestic judicial review, foreign law enforcement officers issuing direct demands for subscriber information will effectively dictate which crimes warrant an intrusion into an individual's privacy. Foreign law enforcement will have the ability to demand, and likely receive, an individual's information for any crime, at any stage in the investigation.

Complying with evidentiary demands based upon what a foreign law enforcement agency believes to be a legitimate intrusion to privacy is a stark contrast to the view of privacy currently embraced by U.S. jurisprudence. While the Fourth Amendment is not directly applicable in a situation in which private companies release subscriber information to a foreign government, as the Fourth Amendment protects only against domestic government intrusion,[48] the Fourth Amendment case law

47. *See generally* R.A.V., 505 U.S. at 377.

48. The Fourth Amendment protects persons against the intrusive acts by officers of the government or those acting at their direction. Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 613–14 (1989). However, there is likely an argument to be made that by ratifying the second additional protocol and enabling direct demands, foreign governments would be acting at the U.S. government's direction.

shows the emphasis that United States places on domestic societal values regarding privacy.

When U.S. courts determine whether an individual's privacy has been infringed upon by law enforcement, they employ one of two dominant tests: a trespass analysis[49] or a reasonable expectation of privacy analysis.[50] Under the reasonable expectation of privacy analysis, courts apply a two-pronged test: (1) whether an individual displayed a subjective expectation of privacy and (2) whether there was an objective expectation of privacy that *society* is willing to protect.[51] It is very possible that, following the Supreme Court's decision in *Carpenter v. U.S.*, a court could find there is a reasonable expectation of privacy in an individual's subscriber data, which would then require a domestic warrant to access.[52] More importantly, however, the reasonable expectation of privacy analysis reflects the understanding that American society should have a determinative role in deciding the balancing act between privacy and law enforcement.[53] Allowing foreign law enforcement officers to effectively make the determination regarding the importance of privacy contradicts the U.S. view of how privacy should be evaluated in the realm of criminal investigations.

Allowing foreign governments to exert greater control of privacy rights will also likely result in a different value judgment regarding privacy in comparison to law enforcement. European countries, many of which are parties to the Budapest Convention, generally take a different approach in balancing law enforcement and privacy. For example, in the United States, the U.S. National Security Agency collected the telephone data of millions of Americans without a warrant following the September 11, 2001 attacks.[54] At least one U.S. court held that the massive data collection was lawful.[55] However, if a similar data collection program was enacted in Europe, the collection would be blatantly illegal.[56] This represents a difference in the approach to law enforcement

49. A search, and a resulting intrusion into an individual's privacy, occurs when police trespass onto an individual's property. U.S. v. Jones, 565 U.S. 400, 409 (2012).

50. There is a reasonable expectation of privacy in an individual's cellphone location data. Carpenter v. U.S., 138 S. Ct. 2206, 2217 (2018).

51. *See, e.g.*, Katz v. U.S., 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

52. This idea has been contemplated by Justice Sotomayor. U.S. v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring). Currently, there is no reasonable expectation of privacy in a user's subscriber information because it has been shared with the internet service provider.

53. *See generally*, Carpenter, 138 S. Ct. 2206; Riley v. California., 573 U.S. 373 (2014); U.S. v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring).

54. Francesca Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609, 610 (2007).

55. ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013).

56. Bignami, *supra* note 55, at 610.

between the United States and Europe. European countries may be less likely to sacrifice an individual's privacy to expedite law enforcement investigations. Further, as discussed *supra*,[57] European countries may be more willing than the United States to sacrifice privacy to prosecute speech crimes.

However, proponents of greater privacy protections could argue that allowing foreign governments to determine which crimes warrant intrusion into an individual's privacy could be a positive development, as European countries generally protect privacy to a greater extent than the United States.[58] For example, the European Union Charter of Fundamental Rights states that "everyone has the right to protection of personal data."[59] Advocates for greater privacy could argue that allowing foreign governments to exert more control could create a global consensus regarding the importance of privacy.

While a resulting global consensus may sound appealing in theory, a consensus may be unlikely to actually develop through the second additional protocol as it is currently drafted. Sixty-six countries are party to the Budapest Convention,[60] and the large number of member states represents a wide variation in the level of privacy protection. Each country that is a party to the Budapest Convention, including the United States, will have the opportunity to play a role in the development of privacy regulation under the additional protocol. Therefore, a risk exists that the European approach, which protects privacy to a greater extent, will not prevail over the approach of other countries which may become a party to the second additional protocol. The more likely result of the second additional protocol is greater legal confusion regarding the tolerable levels of privacy intrusion.

Allowing foreign governments to determine when a user's data will be disclosed is further concerning due to the disclosure's high level of privacy intrusion. The explanatory report to the draft protocol claims that disclosure will not reveal private information concerning the individual, stating that "[subscriber information] does not allow precise conclusions concerning the private lives and daily habits of individuals

57. *See supra* Section II A 3.

58. Ronald J. Krotoszynski, Jr., *Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis*, 56 WM. & MARY L. REV. 1279, 1289 (2015).

59. Charter on Fundamental Rights of the European Union, art. 8, Oct. 26, 2010, 2010 O.J. (C 83) 389.

60. *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUR. (2021), https://www.combattingcybercrime.org/files/virtual-library/international-cooperation/chart-of-signatures-and-ratifications-of-treaty-185-%e2%80%93convention-on-cybercrime-%28status-as-of-16-06-2016%29.pdf.

concerned."[61] However, in reality, sensitive personal information is at risk.[62] Significant information can be gleaned about an individual's daily life from just their IP address, making these direct requests particularly intrusive on an individual's privacy.[63] For example, an IP address can show an individual's interests, personal intimacies, and beliefs.[64] The amount of information that can be revealed through the process of direct disclosure necessitates more protection than is currently provided by the draft second protocol.

III. Complying with requests on a case-by-case basis

The other likely scenario, in which companies respond to some evidentiary requests from foreign law enforcement on a case-by-case basis, presents a different issue: the creation of a private regulatory regime. When internet service providers have the ability to fight certain requests and government sanctions, they can pick and choose which investigations are worth divulging their users' data. The lack of a dual criminality requirement removes legal standards by which companies can base their decisions about whether or not to release a user's data, making their decisions all the more arbitrary. The determinations that these private companies make have the ability to create a large impact on both speech and privacy. Therefore, the decisions should instead be left to a democratic process and an accountable judicial system.

A. *Speech*

If the second additional protocol were to be implemented as currently drafted, the protocol would allow the internet service providers with the most resources to establish their own regulatory regime regarding what type of speech should be tolerated online.

The risk of a private regulatory regime is particularly relevant in the United States given the level of control that internet service providers

61. Draft Provisions, *supra* note 17, § 4.2(3).

62. EuroISPA, Council of Eur., EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention 2 (2019), https://rm.coe.int/euroispa-s-comments-to-draft-provisions-2nd-add-protocol-final/168098bcab [hereinafter EuroISPA's comments].

63. Internet Serv. Providers Austria, Council of Eur., ISPA Austria's Contribution to the Public Consultation on the Provisional Text of the Second Additional Protocol to the Budapest Convention on Cybercrime 3 (2019), https://rm.coe.int/ispa-comments-second-additional-protocol-budapest-convention/168098bba8.

64. *See* U.S. v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); Benedik v. Slovenia, App. No. 62357/14, ¶ 109 (Apr. 24, 2018), http://hudoc.echr.coe.int/eng?i=001-182455; EuroISPA's comments, *supra* note 63, at 2.

enjoy on their platforms, as compared to their counterparts in Europe. The United States is resistant to any content regulation of the press, and by analogy, will likely be resistant to regulate content on social media platforms and internet service providers.[65] In contrast, European countries place civil and criminal liability on social media companies for failure to control certain types of speech on their platforms through EU Directives, EU Internet Response Units,[66] and the ICT Code of Conduct to Quickly Remove Hate Speech.[67] While the U.S. government can regulate conduct through public pressure, particularly in the sphere of national security,[68] the private sector in the United States plays a large role in determining what can and cannot be published on the internet.[69]

The power of private decision-making in the context of content moderation has already been displayed. For example, the CEO of CloudFare, a web infrastructure provider, decided to blanketly remove the material of white nationalists from his platform and later stated, "I woke up in a bad mood and decided that someone shouldn't be allowed on the internet. No one should have that type of power."[70] Given the extremely complicated nature of speech on the internet and the potential global repercussions of removing certain speech,[71] decisions about acceptable online speech should be regulated by representative government processes as opposed to "the in-house counsel of a few giant, young corporations."[72]

The lack of governmental oversight and control over technology companies, combined with the lack of a dual criminality requirement in the draft protocol, will allow private companies to determine whether or not to release a user's information based upon what speech the company decides is worthy of punishment. Although foreign law enforcement officers are not required to provide a statement of the facts in the evidentiary orders to internet service providers,[73] the officers must include a description of the charge for which they are seeking

65. *See* Kyle Langvardt, *Regulating Online Content Moderation*, 106 GEO. L.J. 1353, 1365–66 (2018). *See generally* Mia. Herald Publ'g Co. v. Tornillo, 418 U.S. 241 (1974).

66. *See generally* Brian Chang, *From Internet Referral Units to International Agreements; Censorship of the Internet by the U.K. and EU*, 49 COLUM. HUM. RTS. L. REV. 114 (2018).

67. *Code of Conduct on Countering Illegal Hate Speech Online*, EUR. COMM'N (May 31, 2016), http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

68. For example, President Obama pressured YouTube to remove an anti-Muslim video following the Benghazi attacks. Langvardt, *supra* note 66, at 1379.

69. *See id.* at 1357.

70. *Id.* at 1358.

71. *See* discussion regarding the chilling effect of speech *supra* Section III A.

72. Langvardt, *supra* note 66, at 1356.

73. Draft Provisions, *supra* note 17, § 4.1(3)-(4).

evidence.[74] The requirements regarding what information must be transmitted to internet service providers include just enough information to be dangerous: the requirements allow private companies to decide when to participate in an investigation solely based on the offense, without having any knowledge of the specific circumstances surrounding the offense.

Furthermore, there is a strong possibility that the decisions of internet service providers regarding what speech should be investigated and, as a likely result, prosecuted, will differ from the requirements of the U.S. Constitution, as reasonable minds differ regarding the balance between the freedom of speech and other rights, such as privacy. It is very possible that a company's leadership will find that they align more naturally with the European approach to speech and grant access to a subscriber's information based upon cases which suit support their policy views. Alternatively, an official determining whether to grant access to a subscriber's data might base her decision simply on the content of the individual's speech, or the group that was speaking, as was the case with the CloudFare CEO. Indeed, it would be difficult to fault an individual for wanting to assist with an investigation into truly offensive and horrific hate speech, despite the fact that the content of the speech and the speaker would be protected by the First Amendment.[75]

The differing of opinions regarding what speech should and should not be online will also lead to inconsistent results. The risk of inconsistent results is increased by the lack of specific definitions in criminal speech statutes. Crimes such as "encouragement of terrorism" are often defined broadly, and the breadth of these definitions creates more opportunities for internet service providers and other actors to use these crimes as cover for taking actions such as takedown policies that interfere with the freedom of speech and expression.[76] The wider the range of possible meanings of these terms, the larger the risk that one person's discretionary interpretation of a crime becomes a global standard, based solely upon that individual's role at a particular internet service provider.[77]

The danger of inconsistent results is exemplified by modifying the original hypothetical posed in the introduction regarding Holocaust

74. *Id.*

75. *See generally* R.A.V., 505 U.S. 377.

76. *See* Chang, *supra* note 67, at 149; Angel Diaz, *Global Internet Forum to Counter Terrorism's 'Transparency Report' Raises More Questions Than Answers*, JUST SEC. (Sept. 25, 2019), https://www.justsecurity.org/66298/gifct-transparency-report-raises-more-questions-than-answers/.

77. Diaz, *supra* note 77.

denial. Imagine that law enforcement agents in Germany are now investigating two incidents of Holocaust denial posted online. The content of the messages is essentially equivalent. However, the individuals who posted these messages employ different internet service providers. The German authorities issue a direct demand for the individual's data to both service providers. One provider complies with the request because that provider believes that posts advocating Holocaust denial should not be allowed on the internet. The German authorities are now able to identify and prosecute one of the individuals. However, the second provider believes that all speech should be allowed on the internet and so refuses to comply with the request. Assuming the second company has the resources to defeat any enforcement action, the German authorities are now unable to collect the necessary evidence. The second individual will likely go unpunished. The result that one individual is punished while another goes free for the same crime, based merely on the belief of a private actor, creates an unfair legal regime filled with uncertainty about what speech will and will not be tolerated online.

If government actors were to make these decisions, voters would be able to hold them accountable through elections. Additionally, passing legislation regarding speech on the internet would require approval from both the House of Representatives and the Senate, along with the approval of the President, preventing one individual from setting a national, or global, agenda regarding speech on the internet. The public further has the option to challenge these decisions in court. The judicial system has the power to block regulation that infringes on the First Amendment. However, when private companies make decisions regarding what should be on the internet, the public does not have the option of voicing their displeasure with the decision, given that users would not even be informed when a company provides their data to law enforcement.[78] Users also cannot hold the individuals making decisions about their data, and, by extension, policy decisions regarding online speech accountable through elections. Voters are instead delegated to the role of users who must abide by boilerplate agreements which are generally non-negotiable.[79] Allowing speech decisions to be made by policy makers avoids the possibility that type of speech allowed on the internet will be dictated by one powerful individual's mood in the morning, as was the case for the CloudFare CEO.[80]

78. *See generally* Draft Provisions, *supra* note 17, § 4.1.

79. Eyal Benvenisti, *Upholding Democracy Amid the Challenges of New Technology: What Role for Global Governance?*, 29 EUR. J. INT'L L. 9, 71 (2018).

80. Langvardt, *supra* note 66, at 1358.

As discussed *supra*[81] the decisions that companies make regarding whether or not to turn over information to a foreign government can have a large impact on speech. The policies these companies set regarding the crimes for which they are willing to provide subscriber information for has the potential to set a global expectation of what speech should or should not be acceptable online. Determining what speech is allowed online is an inappropriate role for a private company, which is not restrained by the U.S. Constitution or accountable to American voters.

B. *Privacy*

The second draft protocol further creates the danger of a private judiciary, as private companies will make determinations about whether or not a certain crime justifies privacy intrusions. Allowing companies to make decisions about privacy is concerning because the draft does not provide legal standards to guide the decision-making process, which lacks accountability, and decisions are made by actors who have an economic interest in the information being shared. This leads to a regime in which private actors, as opposed to an established judiciary system, are making key decisions involving individuals' rights.

1. Lack of Legal Standards

The draft protocol does not provide legal standards by which internet service providers can assess the legitimacy of a request for subscriber information and does not allow companies to have the information necessary to make a competent decision. As one commentator phrased it, the direct demand on internet service providers "undermines the essential duties of national judicial authorities to ensure that the rights of its citizens are not infringed, compromised[,] or undermined."[82] The direct demand requirement goes around the judiciary and essentially means that private internet service providers "are the last line of defense against user's rights against abuses."[83] Circumventing a judiciary violates basic privacy rights.[84]

The draft protocol instead leaves the role of ensuring that individual rights are protected to the internet service providers, which may not have the resources or legal expertise to determine if an evidence production order complies with U.S. privacy standards, either statutory or

81. *See supra* Section II A.

82. COUNCIL OF BARS AND LAW SOCIETIES OF EUR., CCBE COMMENTS 3 (2019), https://rm.coe.int/ccbe-written-comments-draft-2nd-additional-protocol-to-the-convention-/168098bc6e [hereinafter CCBE Comments].

83. Joint Civil Society Response, *supra* note 15, at 3.

84. CDT Comments, *supra* note 33, at 5.

constitutional. Even if a company were to have the necessary resources to create internal policies and guidelines for disclosure of data to foreign law enforcement, the internet service provider may not be able to apply those policies to a request or even realize the implications of complying with a request, given that governments are not required to provide a summary of the facts regarding the crime for which they are gathering evidence.[85]

The draft protocol imagines a process that is analogous to Europe's "right to be forgotten" policy, which has also been criticized for creating a private judiciary system.[86] Similar to the direct demand requirement under the draft protocol, under the "right to be forgotten" policy; an individual can make a request directly to a company, such as Google, asking that that the company remove certain information about the individual by completing a form. The company will then decide whether or not to remove certain online posts based on whether the company believes the content is inadequate, irrelevant, no longer relevant, or excessive.[87] However, deciphering whether a post in question fits in one of these categories often requires a more significant investigation into the facts than what can be provided on an online complaint form.[88] In his critique of the "right to be forgotten" process, Professor Eldar Haber states:

> the decider needs to obtain background information on the data subject and the consequences surrounding the request. It may also require depositions, testimonies, and other types of evidence . . . there may also be another side to the story, which the search engines will not be aware of. It would be highly difficult, if not impossible, to evaluate such requests, when the only information examined is provided by the requester, and the evaluators rely only on what the requester claims to be accurate . . . the process eventually leads to information gaps caused by imperfect or asymmetrical information, which could be partially resolved under a judicial proceeding.[89]

Given the similarities between the draft protocol and the "right to be forgotten" policy, Haber's critique applies forcefully against the direct

85. *Id.* at 4.
86. *See generally* Eldar Haber, *Privatization of the Judiciary*, 40 SEATTLE U. L. REV. 115 (2016).
87. *Id.* at 142.
88. *Id.*
89. *Id.* at 142–43.

demand requirement. Analogous to the individual going straight to a company to request that a post be removed as opposed to a judge, foreign law enforcement officers will also be going directly to internet service providers without going through the judiciary under the draft protocol. Furthermore, similar to the limited information provided to companies on an online form under the "right to be forgotten" policy, foreign law enforcement will provide only limited information to internet services providers when requesting information. Companies will not have the ability to understand the context in which they are providing a user's information and will be relying solely on the belief in the good faith of the foreign law enforcement officers.

However, the draft protocol does imagine a system that would essentially function as a warrant. When law enforcement officers apply for a warrant domestically, the magistrate issuing the warrant receives information only from law enforcement. The magistrate does not get information from the potential defendant and is often relying on law enforcement's good faith. Nonetheless, the magistrate can press an officer for more supporting information and will certainly demand more information than just the name of the crime being investigated.

The issue with the lack of legal standards is displayed by again modifying the original hypothetical regarding Holocaust denial. Imagine that the company receiving the demand for evidence has created a policy that the company will respond to requests for crimes that constitute "hate speech." When the company receives the evidence demand, the company will only be told that the German authorities are investigating the crime of Holocaust denial. Without a statement of the facts, or having access to the original post, how is the company to know if the Holocaust denial constitutes hate speech in this instance?

The process for decision making created by the draft protocol places private companies in a position where they must guard a significant privacy right without any legal guidance or a body of facts to support the decision-making process. The absence of a legal framework creates the risk of arbitrary determinations that lack a factual foundation.

2. Lack of Accountability

Furthermore, once a private company makes a decision to release the information, companies are not held accountable for the decision, as the second additional protocol does not allow users to appeal a decision. Instead, internet service providers are shielded from liability for

complying with a request.[90] Similar critiques arise when platforms such as Twitter or Facebook remove content. Under the critique of Professor Hannah Bloch-Wehba, allowing companies to make such decisions about content or a users' data is two steps removed from a democratic process because the decision is made by unelected, non-state actors and occurs outside traditional accountability mechanisms.[91] Other academics have characterized internet service providers and other technology platforms as "politically unaccountable technology oligarchs that exercise state-like censorship powers."[92]

In the judiciary realm, judges are held accountable for their decisions, *inter alia*, through an appeals process. In a traditional judiciary system, the appeals process protects against arbitrary or erroneous application of the law, promotes the development of legal doctrine, and assists in standardizing outcomes for similarly situated individuals.[93] All of the risks that the appeals process protects against are present in the regime imagined by the draft protocol: companies may arbitrarily or erroneously apply the law given the lack legal standards and factual knowledge basis, and similarly situated individuals may very well receive different results based on the internet service provider they employ. Yet, the draft protocol does not provide any mechanism whereby a user can challenge the company's decision to disclose information or a company can challenge an evidentiary request from foreign law enforcement. The lack of an appellate system thereby enhances the risk of arbitrary privacy protection.

3. Economic Interests Create a Conflict of Interest

Additionally, internet service providers are private for-profit actors who have an economic interest in their users' data. The economic interest raises potential doubt as to their commitment to their users' privacy rights.[94] Private technology companies maximize their profits through expanding their market shares and ad revenues,[95] meaning that the level to which companies are willing to protect privacy could vary based

90. Draft Provisions, *supra* note 17, §§ 4.2(7), 5.2(6).
91. Bloch-Wehba, *supra* note 38, at 66–67.
92. Langvardt, *supra* note 66, at 1358; *see id.* at 60–61.
93. Haber, *supra* note 87, at 151.
94. Benvenisti, *supra* note 80, at 71.
95. *Id.* at 74.

on where their financial interests lay at the time.[96] If a company is looking to expand its user base, the company may well act as an "information fiduciary" that has duties of trust and loyalty to its users,[97] and more adamantly defends users' privacy rights. This is already exemplified by Apple's recent publicity campaign, which prominently features its commitment to keep users' information private.[98] However, while this strategy may adequately protect a user's right of privacy, the company very well may impede what would otherwise be considered a necessary, lawful intrusion into a user's privacy in order to prevent a serious crime.

IV. Recommendations

If the protocol were to be ratified as currently drafted, the second additional protocol would create either over-regulation by foreign authorities or the development of a private regulatory regime. For these reasons, the United States should not ratify the protocol as it currently stands. However, the United States increasingly seeks electronic evidence stored abroad;[99] thus, the United States should maintain its interest in improving the MLA process. Therefore, the United States should recommend changes either to the draft language of the second additional protocol or to the reservations allowed to protocol.

The United States should propose language changes which require domestic judiciary review of evidentiary requests, dual criminality, and the inclusion of supporting factual background information in evidentiary requests. The United States might also consider including a process by which internet service providers may appeal an evidentiary request, without threat of punishment. An appeals process may relieve private companies from the pressure to comply with every evidentiary request.

However, the United States may face resistance to the proposed changes, as other party states may argue that the proposed changes frustrate the object and purpose of the protocol, in violation of the Vienna Convention on the Law of Treaties.[100] Other parties to the Budapest Convention may

96. *See* Haber, *supra* note 87, at 154–55.

97. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 45 U.C. Davis L. Rev. 1183, 1221 (2016).

98. Mike Wuerthele, *"Privacy. That's iPhone" Ad Campaign Launches, Highlights Apple's Stance on User Protection*, Apple Insider (Mar. 14, 2019), https://appleinsider.com/articles/19/03/14/privacy-thats-iphone-ad-campaign-launches-highlights-apples-stance-on-user-protection.

99. Mulligan, *supra* note 5, at 15.

100. *See* Vienna Convention on the Law of Treaties, arts. 18, 19(c), May 23, 1969, 1155 U.N.T.S. 331. It should further be noted that the United States is a signatory, but not a party to the Vienna Convention on the Law of Treaties. U.N. Treaty Collection, *Law of Treaties*, United Nations 1, 11

argue that, as the second additional protocol was designed to create a more efficient MLA process[101] and the proposed language changes will likely slow the MLA process, the changes frustrate the object and purpose of the second additional protocol.

Nonetheless, the United States should propose language changes to either the main text of the protocol or the allowable reservations. The United States may have more success proposing an acceptable reservation to the second additional protocol, so the recommended language changes are phrased as a permissible reservation. Given the importance of addressing all the major deficiencies in the proposed protocol, the proposed language should be read together as one reservation. The proposed language is broken down here in order to show how the United States could address each of the deficiencies of the proposed protocol.

First, regarding domestic judicial review, the United States should suggest:

> At the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, a Party may – with respect to orders issued to service providers in its territory – make the following reservation: the order under Article [x], paragraph [x] must be approved and issued by, or under the supervision of, a domestic judicial authority of the requested Party.

Second, regarding a dual criminality component, the United States should suggest: "Should a Party require the order be issued by, or under the supervision of, a domestic judicial authority, the domestic judicial authority will deny an order if the condition of dual criminality is not fulfilled."

Third, regarding the inclusion of supporting information in evidentiary request, the United States should suggest:

> Should a Party require the order be issued by, or under the supervision of, a domestic judicial authority, the domestic judicial authority will deny an order if the application for the order does not include supporting information. 'Supporting information' must include a summary of the facts relating to the

(2021), https://treaties.un.org/doc/Publication/MTDSG/Volume%20II/Chapter%20XXIII/XXIII-1.en.pdf.

101. Enhanced International Cooperation, *supra* note 16, at 2.

> investigation, the requesting party's domestic legal grounds that empower the authority to issue the order, and applicable penalties of the crime being investigated. 'Supporting information' may include any other information that the requesting party considers relevant.

Finally, regarding a proposed appeals process, the United States should suggest:

> After an order is approved by a domestic judicial authority and issued to the appropriate internet service provider, the internet service provider receiving the order may appeal the order if the internet service provider believes that the domestic judicial authority has incorrectly evaluated the order and the order does not comply with domestic law or constitutional requirements.

The United States should not sign the additional protocol without the inclusion of these language changes or equivalent language changes.

V. Conclusion

As the world increasingly moves online, speech and privacy rights have become more global in nature. As speech and privacy rights become more global, the protection of these rights becomes even more complex and important. Therefore, complex decisions regarding speech and online privacy should be left to accountable, representative government systems. However, the MLA reform created by the second additional draft protocol will assign the decision-making role regarding speech and privacy protection to either foreign governments or the private sector. The shift in power risks foreign law enforcement control over speech and privacy values and the creation of an unaccountable private regulatory regime. For these reasons, the United States should not sign the proposed protocol as it stands.

However, given the ever-increasing importance of electronic evidence and the issues with the current MLA process, which hinder necessary criminal investigations, the United States should consider proposing alternatives to the current draft. The United States should propose language changes that require domestic judicial review of evidentiary orders, fulfillment of dual criminality, the inclusion of supporting information in evidentiary orders, and an appeals process. These changes will properly shift power to the domestic representative

governments and judicial systems to make determinations regarding online speech and the balance between effective law enforcement and privacy. If the changes are implemented, the United States might seriously consider signing and ratifying the additional protocol.