Masthead Logo

Volume 9 | Issue 2 Article 5

5-22-2019

The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform

Christine Galvagna
Global Public Policy Institute, Berlin

The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform

Cover Page Footnote
German Chancellor Fellow, Global Public Policy Institute, Berlin. The author can be contacted at cgalvagna@gppi.net.

THE NECESSITY OF HUMAN RIGHTS LEGAL PROTECTIONS IN MUTUAL LEGAL ASSISTANCE TREATY REFORM

CHRISTINE GALVAGNA*

INTRODUCTION

Two things differentiate a surveillance state from a non-surveillance state: the ease of government access to personal data and the strength of a

* German Chancellor Fellow, Global Public Policy Institute, Berlin. The author can be contacted at cgalvagna@gppi.net.

country's human rights legal framework. Both are being profoundly altered by recent transnational legal efforts, collectively called mutual legal assistance (MLA) treaty (MLAT) reform, aimed at facilitating cross-border data access for law enforcement. MLATs enable law enforcement agencies to obtain evidence located in foreign countries, including personal data and other electronic evidence.[1] Reform efforts are necessitated by the failure of slow and complex traditional MLA procedures to meet growing law enforcement demands, as well as uncertainty about jurisdiction over data results in international disputes. However, in the rush to mollify law enforcement agencies, and the attention demanded by complex procedural and jurisdictional issues, human rights protections tend to be an afterthought. If this continues, governments may unwittingly produce the conditions that give rise to surveillance states all over the world.

The desire to reduce legal complications associated with cross-border data access is understandable. A criminal investigator in country A, for example, may need access to the content of an e-mail sent by one of its nationals via Google's Gmail, but may wait for months, while the request percolates through the Department of Justice (DOJ) and the United States (U.S.) federal court system. Governments in country A and the U.S. may disagree over which has jurisdiction over the data—country A may have jurisdiction over the suspect and location of the crime, while the data may be held by a U.S. company subject to U.S. jurisdiction. This may be all the more complicated when the data is stored on a server in country B, which may argue that the data's physical presence in its territory gives neither country A nor the U.S. jurisdiction over it.

Some states respond by empowering themselves to circumvent the MLA process with problematic new domestic policies. One tactic is mandated data localization, which forces service providers to store user data on servers within a state's territory. This undermines Internet and web openness, which is crucial to its functioning. Another tactic is for a government to grant itself the legal authority to demand access to data regardless of where the data are stored. This arguably undermines the principle of state sovereignty.

MLAT reform is necessary to disincentivize these problematic unilateral measures, reinforce state sovereignty, and remove barriers to effective law enforcement. Yet, to varying degrees, recently proposed and enacted measures, including the U.S. Clarifying Lawful Use of Overseas Data (CLOUD) Act, the European Union's (EU) e-Evidence proposal, and the potential Second Additional Protocol to the Council of Europe's Convention on Cybercrime (Budapest Convention), would expedite access at the expense of legal norms protecting state sovereignty and procedures designed to protect personal data, privacy, and other human rights interests.[2] Only one proposal, a draft legal instrument for an International

---

[1] *See generally*, Mailyn Fidler, *MLAT Reform: Some Thoughts from Civil Society*, LAWFARE (Sept. 11, 2015), https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society; Greg Nojeim, *MLAT Reform: A Straw Man Proposal*, CTR. FOR DEMOCRACY & TECH. (Sept. 3, 2015), https://cdt.org/files/2015/09/2015-09-03-MLAT-Reform-Post_Final-1.pdf; Arthur Rizer & Anne Hobson, *Cross-Border Data Requests: Evaluating Reforms to Improve Law Enforcement Access*, RSTREET (Nov. 2017), http://2o9ub0417chl2lg6m43em6psi2i.wpengine.netdna-cdn.com/wp-content/uploads/2017/11/120.pdf.

[2] Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, 132 Stat. 348 (2018). This Act is also known as the CLOUD Act. The two elements of the e-Evidence proposal are a Proposal for a Regulation of the European Parliament and of the Council on European Production

Data Access Warrant, introduced by the U.N. Special Rapporteur on the right to privacy, adequately addresses human rights issues, wait-times for law enforcement, and state sovereignty.[3]

While MLAT reform revolves around a set of relatively technical and esoteric legal issues, policymakers must not lose sight of the potentially Orwellian impact that poorly-designed MLAT reform could have on human rights and democratic institutions. Any long-term solution must compensate for lost legal protections to ensure that expanded government data collection powers are not abused.

I. THERE IS A LEGITIMATE AND PRESSING NEED FOR MLAT REFORM

A. *THE U.S. MLA PROCESS IS TOO SLOW AND INEFFICIENT*

MLA processes in the U.S., where most computer records are requested, are too slow and inefficient to meet foreign law enforcement demands.[4] MLA requests for data held by U.S. companies typically entail months-long wait-times, impeding law enforcement efforts all over the world.

Foreign governments utilize the U.S. MLA process to obtain warrants and court orders necessary to access data controlled by U.S. tech companies.[5] The Electronic Communications Privacy Act (ECPA) generally prohibits a U.S. company from providing communications content to a foreign government outside of the MLA process.[6] While companies are free to disclose non-content data, they often refrain from doing so, necessitating use of the MLA process.[7]

The U.S. MLA process is complex. To obtain a U.S. warrant or court order, a foreign law enforcement agency must first seek approval from a specialized domestic "central authority."[8] If approved, the request is sent to

---

and Preservation Orders for electronic evidence in criminal matters. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM (2018) 225 final (Apr. 17, 2018) [hereinafter *Draft Regulation*]; *Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, COM (2018) 226 final (Apr. 4, 2018) [hereinafter *Draft Directive*]; Council of Europe, *Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*, CYBERCRIME CONVENTION COMM. (June 9, 2017), https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b [hereinafter *Terms of Reference*]; Convention on Cybercrime (Budapest Convention), Nov. 23, 2001, E.T.S. 185 [hereinafter Budapest Convention]; Joseph A. Cannataci (United Nations (U.N.) Special Rapporteur on the right to privacy), *Working Draft Legal Instrument on Government-led Surveillance and Privacy, Version 0.7* (Feb. 28, 2018), https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf [hereinafter *Draft Legal Instrument*].

[3] *Draft Legal Instrument*, *supra* note 2.

[4] Council of Europe, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, CYBERCRIME CONVENTION COMM. 61–81 (Dec. 3, 2014), https://rm.coe.int/16802e726c [hereinafter *T-CY Assessment Report*].

[5] *See generally* STEPHEN P. MULLIGAN, CONG. RESEARCH SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT 12–14 (2018).

[6] 18 U.S.C. § 2702(a) (2018).

[7] 18 U.S.C. § 2702(c)(6); *Commission Staff Working Doc. Impact Assessment*, at 27, SWD (2018) 118 final (Apr. 17, 2018) [hereinafter *Impact Assessment*].

[8] TIFFANY LIN & MAILYN FIDLER, BERKMAN KLEIN CTR., CROSS-BORDER DATA ACCESS REFORM: A PRIMER ON THE PROPOSED U.S.-U.K. AGREEMENT 2–3 (2017); DEP'T OF JUST. CRIM. DIV., FY 2016 PRESIDENT'S BUDGET [hereinafter 2016 BUDGET].

the DOJ's Office of International Affairs (OIA), the U.S. central authority, which determines whether it meets U.S. legal requirements, such as whether the factual basis for suspicion amounts to probable cause.[9] Once satisfied, OIA sends the request to a U.S. Attorney's Office, which brings the case before a federal magistrate judge.[10] If the judge approves the request, he or she issues a warrant or order to the relevant company.[11] The company then sends the data to OIA, which determines whether it meets data minimization and human rights requirements.[12] OIA then sends the data to the foreign government's central authority, which supplies it to the law enforcement agency.[13]

In addition to the complexity of this process, OIA's workload contributes to slow response times. Annual MLA requests for computer records increased by over 1,000% between the years 2000 and 2014.[14] Response times were roughly six to twenty-three months in 2014.[15] In the 2016 fiscal year, there was an MLA request backlog, including non-computer record requests, of 13,421 cases, though this has been reduced to 9,038 as a result of a one-off budget increase for additional staff.[16] Currently, EU member states typically wait between one and six months for access.[17]

Non-content data may be obtained directly from U.S. companies, outside of the MLA process. An exception in ECPA permits companies to disclose non-content data to foreign governments at their discretion.[18] Despite receiving many more requests than OIA, U.S. companies comply with requests far more quickly. For example, EU member states sent around 120,000 requests to Google, Facebook, Microsoft, Apple, and Twitter in 2016, with a typical response time of around eleven to thirty days.[19]

This discrepancy—a wait-time of eleven to thirty days for direct requests on the one hand, and a wait-time of one to six months for MLA requests, on the other—frustrates foreign governments and undermines their criminal justice systems.[20]

---

[9] LIN & FIDLER, *supra* note 8, at 2.

[10] *Id.* (though OIA may request data in a federal court without the assistance of a U.S. Attorney, it often lacks the resources to do so); 18. U.S.C. § 3512 (1995); 2016 BUDGET, *supra* note 8, at 24.

[11] LIN & FIDLER, *supra* note 8, at 2.

[12] *Id.* at 3.

[13] *Id.*

[14] 2016 BUDGET, *supra* note 8, at 22–23.

[15] *T-CY Assessment Report*, *supra* note 4, at 123 (describing a survey of thirty-six parties and three observer states).

[16] 2016 BUDGET, *supra* note 8, at 22 (noting that seventy-seven additional attorneys and paralegals were requested to be hired with the one-off budget increase of $32,111,000).

[17] *Impact Assessment*, *supra* note 7, 263–64 (describing self-reported wait times, as measured by the mode, for access to content and non-content data through non-EU government authorities; the numbers mainly reflect United States' requests).

[18] 18 U.S.C. § 2702(c)(6) (2018); 18 U.S.C. § 2711 (prohibiting disclosure to governmental entities, which means only U.S. governmental entities*); Impact Assessment*, *supra* note 7, at 14 (discussing how non-content data is the most commonly sought category of data). Most state parties to the Budapest Convention do not permit service providers to voluntarily disclose non-content data.

[19] *Impact Assessment*, *supra* note 7, at 194 (While this figure is calculated with both U.S. and non-U.S. service provider response times, the number largely reflects U.S. companies, as they receive the majority of requests.).

[20] *Id.*; *see also* Andrew K. Woods, *Interview: The British Perspective on the Cross-Border Data Problem*, LAWFARE (Feb. 7, 2018), https://www.lawfareblog.com/interview-british-perspective-cross-border-data-problem.

B. *UNILATERAL MEASURES*

Unsurprisingly, governments have begun to circumvent the U.S. MLA process. Some now require service providers to store data within their respective jurisdictions, rendering the MLA process irrelevant, while others have given themselves authority through domestic law to demand the production of data stored anywhere.

Data localization is one policy response to slow MLA processes.[21] Germany and Russia, for example, require companies to store at least some categories of personal data on servers located within state boundaries.[22] While data localization allays more immediate concerns about response times, it also generates more consequential problems. First, data localization undermines Internet and web openness.[23] The imposition of territorial borders restricts a company's ability to manage data traffic in ways that enhance efficiency, security, and interoperability.[24] Second, data localization can be used as a pretext for more aggressive surveillance and censorship.[25]

Another policy response, the use of domestic law to empower law enforcement authorities or courts to demand its nationals' data regardless of where the data is stored, poses its own problems. While the argument that jurisdiction over data should not be determined by physical location may be sound, it lacks international consensus.[26] Absent this consensus,

---

[21] *See, e.g.*, Jonah F. Hill and Matthew Noyes, *Rethinking Data, Geography, and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls*, NEW AM. (2018), https://www.newamerica.org/documents/2084/Rethinking_Data_Geography_Jurisdiction_2.21.pdf ; Peter Swire, *Why Cross-Border Government Requests for Data Will Keep Becoming More Important*, LAWFARE (May 23, 2017), https://www.lawfareblog.com/why-cross-border-government-requests-data-will-keep-becoming-more-important.

[22] *See* Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, published Dec. 10, 2015, BUNDESGESETZBLATT [BUNDES GBL] (Ger.) (*Law on the Introduction of a Storage Obligation and a Maximum Storage Period for Traffic Data*) [translated]; *Personal Data of Russian Citizens Required to be Stored in Data Centers Located in Russia*, SQUIRE PATTON BOGGS (2014), https://www.squirepattonboggs.com/~/media/files/insights/publications/2014/08/personal-data-of-russian-citizens-required-to-be/files/14492--ipt-personal-data-of-russian-citizens--ne/fileattachment/14492--ipt-personal-data-of-russian-citizens--ne.pdf.

[23] Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet*, CA. INT'L L. CTR. 1, 4 ("By creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe. The Internet is a global network based on a protocol for interconnecting computers without regard for national borders. Information is routed across this network through decisions made autonomously and automatically at local routers, which choose paths based largely on efficiency, unaware of political borders. Thus, the services built on the Internet, from email to the World Wide Web, pay little heed to national borders. Services such as cloud computing exemplify this, making largely invisible to users the physical locations for the storage and processing of their data. Data localization would dramatically alter this fundamental architecture of the Internet.").

[24] *See generally* Erica Fraser, *Data Localisation and The Balkanisation of the Internet*, 13 SCRIPTED 359, 363 (2016), https://script-ed.org/wp-content/uploads/2016/12/13-3-fraser.pdf; Dillon Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE (May 22, 2017), https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.

[25] *See, e.g.*, Adam Taylor, *Russia Moves to Block Professional Networking Site LinkedIn*, WASH. POST (Nov. 17, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/11/17/russia-moves-to-block-professional-networking-site-linkedin/?utm_term=.10f8ce92e2a6 ("The aim of this law is to create . . . (another) quasi-legal pretext to close Facebook, Twitter, YouTube and all other services . . . The aim is surveillance, obviously—to make servers of the companies accessible to the Russian national system of online surveillance . . . and also to get the Internet giants effectively landed in Russia." (citations omitted)).

[26] *See generally* DAN JERKER B. SVANTESSON, SOLVING THE INTERNET JURISDICTION PUZZLE (2017).

direct access to cross-border data will generate confusion and international discord following real or perceived violations of state sovereignty.[27]

C. *SOVEREIGNTY AND EXTRATERRITORIALITY*

The mismatch between the traditional territorial conception of state sovereignty in international law, and the non-territorial nature of the web and Internet, results in uncertainty and disagreements about which state has jurisdiction over sought-after data.

Generally, a state has exclusive jurisdiction in law enforcement matters within its territorial borders.[28] The government of one state may not exercise its law enforcement powers within the territory of another state absent the second state's permission.[29] Absent permission, if one state compels an entity to hand over data stored in another state for a law enforcement investigation in the first state, it would arguably be an impermissible exercise of extraterritorial jurisdiction.[30]

In contrast, the Internet and web are generally non-territorial.[31] The data storage practices of tech companies tend not to follow jurisdictional boundaries. Not only are data stored in multiple jurisdictions, but their locations shift over time, and they can be duplicated or split into fragments.[32] Decisions about which server(s) will host a user's data depend on the user's location, the type of data, and cost considerations, among other things.[33] Given that data sought in investigations are stored in a dynamic, borderless way, states may disagree over which has jurisdiction over the data and authority to compel their disclosure.[34] Confusion about jurisdiction may cause one state to unwittingly violate the sovereignty of another.[35]

When the U.S. government demanded that Microsoft hand over data stored in Ireland outside of the MLA process, Microsoft argued that this would be "the same as if U.S. agents bearing a warrant directed Hilton to send a housekeeper into a hotel room in Dublin, photograph a guest's papers, and email the copies to Washington. It is the execution of a search

---

[27] Brief for Respondent at 4, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 14-2985) (arguing that "the presumption against extraterritoriality . . . ensures that courts do not trigger international discord—like the outcry that the Government's order to Microsoft has prompted from foreign leaders around the world.").

[28] HANS KELSEN, PRINCIPLES OF INTERNATIONAL LAW, 212–13 (2003).

[29] *Id.* at 212 (stating that, "coercive acts . . . must not be executed on the territory of another state without the latter's consent. Without such consent they constitute a violation of international law.").

[30] *See, e.g.*, Brief for Respondent, *supra* note 27, at 37–44 (arguing that the "international discord that has erupted, and the potential for conflict with foreign laws, confirm that the warrant entails an impermissible extraterritorial application of the [Stored Communications Act, a portion of ECPA].").

[31] *See generally* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. REV. 317, 336 (2015) (discussing how a sovereignty-based model of internet governance "would be legally simple, but so far, it is not descriptively accurate. States appear generally unable to secure their cyber borders like they secure their physical territory. There is basically one global Internet, not individual national internets. Imposing a sovereignty-based model for cyberspace would thus mark a major change from the status quo and would fundamentally after the domain being governed."); *Internet Invariants: What Really Matters*, INTERNET SOC. (Feb. 3, 2012), https://www.internetsociety.org/internet-invariants-what-really-matters/; *Reisman*, *supra* note 24.

[32] Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 365–78 (2015); Reisman, *supra* note 24.

[33] Daskal, *supra* note 32; Fraser, *supra* note 24, at 362–68.

[34] Reisman, *supra* note 24.

[35] *See, e.g.*, Brief for Respondent, *supra* note 27, at 37–44.

warrant in a place outside the United States."[36] The resulting court challenge drew attention to the fact that Microsoft—like other private companies—is routinely forced to be the arbiter of fundamental principles of international law, conflicts of law concerning fundamental rights, and strong political pressure.[37] Given that Microsoft is a private company, this is not ideal.

Thus, there is a pressing need for MLAT reform. Yet most proposals are problematic, because they streamline access by weakening legal safeguards against abuse.

II. MLAT REFORM IS NEVERTHELESS CONCERNING

Despite the need for MLAT reform, most proposals are concerning because they accelerate data access by eliminating or paring down procedural protections for online privacy, data protection, and other fundamental rights. The resulting legal frameworks may be inconsistent with states' obligations under international human rights law and increase the risk of abuses.

A. *STATES' INTERNATIONAL OBLIGATIONS IN CROSS-BORDER DATA ACCESS*

Longstanding principles governing the right to privacy, combined with emerging standards applicable to contemporary electronic privacy and data protection, limit government discretion to collect personal data for law enforcement purposes.[38] Government interference with privacy or data protection rights must, first, be necessary to achieve a legitimate aim.[39] Second, the interference must be proportionate to that aim, in that it appropriately balances the state's interest in obtaining data with the seriousness of the interference with the subject's privacy and data protection rights.[40] Third, the interference must be in accordance with the law, meaning it has a basis in domestic law that is both compatible with the rule of law generally and is also sufficiently detailed for its consequences to be foreseeable.[41]

Fourth, the interference must be accompanied by adequate safeguards to prevent arbitrary or abusive practices.[42] Legal instruments governing data collection and other surveillance methods must describe the nature of offenses that may justify surveillance; define the categories of people who may be surveilled; limit the duration of surveillance; and describe

---

[36] *Id.* at 33.

[37] *Id.*

[38] *See generally Case of Roman Zakharov v. Russia (Application no. 47143/06)*, HUDOC (2015), http://hudoc.echr.coe.int/eng?i=001-159324 [hereinafter *Zakharov v. Russia*]; Joined cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen, Sec'y of State for Home Dep't v. Watson, 2016 EUR-Lex CELEX LEXIS 970, at ¶¶ 94–96, 103–12 (Dec. 21, 2016); Human Rights Council, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter The Right to Privacy]; Human Rights Council, The Right to Privacy in the Digital Age: Advance Edited Version, U.N. Doc. A/HRC/39/1 (Aug. 3, 2018) [hereinafter The Right to Privacy: Advanced].

[39] *See* The Right to Privacy: Advanced, *supra* note 38.

[40] *Id.*

[41] *Id.*

[42] *Id.*; *Zakharov v. Russia*, *supra* note 38, at ¶ 231.

procedures for examining, using, and storing data obtained, precautions for sharing data with other parties, and the circumstances in which data must or may be destroyed. [43]

Fifth, the interference must be subject to adequate oversight.[44] Oversight may take place before, during, or after data collection.[45] It must be effective.[46] For example, oversight authorities must have access to all relevant information and have the power to terminate breaches of applicable rules.[47] It must also be continuous, subject to public scrutiny, and not give rise to conflicts of interest.[48] Conflicts of interest are especially likely to arise where there is an inadequate separation of powers; for example, when prosecutors are tasked with both authorizing surveillance and prosecuting cases based on this evidence.[49]

Ideally, oversight includes prior merits-based judicial authorization. In comparison to the executive and legislative branches, the judiciary is best-positioned to provide independent, impartial, and procedurally proper decisions about the necessity and proportionality of interferences with fundamental rights.[50] According to the Council of Europe's Venice Commission, as quoted by the European Court of Human Rights,

> there is an obvious advantage of requiring prior judicial authorization for special investigative techniques, namely that the security agency has to go 'outside of itself' and convince an independent person of the need for a particular measure. It subordinates security concerns to the law, and as such it serves to institutionalize respect for the law. If it works properly, judicial authorization will have a preventive effect, deterring unmeritorious applications and/or cutting down the duration of a special investigative measure.[51]

Additionally, an authorizing body must verify that there is a sufficient factual showing to support a "reasonable suspicion" against the target to justify surveillance.[52] Bodies in other branches of government may be

---

[43] The Right to Privacy, *supra* note 38, at ¶ 28.

[44] *Id.*; The Right to Privacy: Advanced, *supra* note 38; *Zakharov v. Russia*, *supra* note 38, at ¶¶ 233–34.

[45] *Zakharov v. Russia*, *supra* note 38, at ¶ 233

[46] *Id.* at ¶¶ 275, 281–82.

[47] *Id.* at ¶ 282.

[48] *Id.* at ¶¶ 230, 275, 281–83.

[49] *Id.* at ¶ 230.

[50] *Id.* at ¶¶ 233, 257, 275; *Case of Szabó and Vissy v. Hungary (Application no. 37138/14)*, HUDOC at ¶ 79 (2016), https://hudoc.echr.coe.int/eng -{"fulltext":["vissy"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-160020"]} (stating: "[i]t is in this context that the external, preferably judicial, *a posteriori* control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance." (citation omitted)) [hereinafter *Case of Szabó and Vissy*]; Joseph A. Cannataci (U.N. Special Rapporteur on the right to privacy), *Report of the Special Rapporteur on the Right to Privacy*, at ¶¶ 25–26, U.N. Doc. A/HRC/34/60 (Feb. 24, 2017) [hereinafter U.N. Doc. A/HRC/34/60].

[51] *Case of Szabó and Vissy*, *supra* note 50, at ¶ 21.

[52] *Zakharov v. Russia*, *supra* note 38, at ¶ 260 ("Turning now to the authorisation [sic] authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security."); *Case of Szabó and Vissy*, *supra* note 50, at ¶ 71 ("There is no legal safeguard requiring [the law enforcement agency] to produce supportive materials or, in

tasked with oversight responsibilities, provided they are sufficiently independent from the executive branch.[53]

Sixth, the interference must be accompanied by a remedy.[54] The remedy must be effective. It must not merely take the form of empty words that leave individuals powerless to seek redress and curb government abuse.[55]

It is important to note that the overall aim of these standards is to limit government discretion. Because of its secrecy and lack of transparency, government surveillance is especially prone to abuse.[56] The abuse of surveillance powers not only threatens the rights of individuals, but can also result in political control and the erosion of democracy.[57] Therefore, it would be "contrary to the rule of law for the discretion granted . . . to be expressed in terms of an unfettered power."[58] By limiting government discretion, these protections reduce the risk of arbitrary interference and abuse.[59] It follows that legal protections that are worded ambiguously, provide toothless oversight powers, or in any other way leave government discretion excessive in practice—regardless of what is written down on paper—fail to satisfy a state's obligations under international human rights law.

B. *HOW THE U.S. MLA PROCESSES PROTECT HUMAN RIGHTS*

The current U.S. MLA process affords subjects of data collection effective legal protections. It entails prior merits-based judicial authorization that is conditioned upon sufficient factual support.[60] Just as the European Court of Human Rights requires "a reasonable suspicion" against an individual, supported by "factual indications for suspecting that person of planning, committing or having committed criminal acts," a U.S. court requires probable cause or "specific and articulable facts showing

---

particular, a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure - and this on the basis of an individual suspicion regarding the target person. For the Court, only such information would allow the authorising [sic] authority to perform an appropriate proportionality test." (citations omitted)); Joined cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen, Sec'y of State for Home Dep't v. Watson, 2016 EUR-Lex CELEX LEXIS 970, at ¶¶ 103–07, 112 (Dec. 21, 2016).

[53] *See, e.g.*, *Zakharov v. Russia*, *supra* note 38, at ¶ 275; Weber v. Germany, App. No. 54934/00 (Eur. Ct. H.R. 2006) (describing a sufficiently independent non-judicial oversight process).

[54] *See Zakharov v. Russia*, *supra* note 38, at ¶ 220.

[55] *See, e.g.*, *id.* at ¶ 298 (finding a remedy insufficient because it relied on knowledge of surveillance, despite a lack of mandatory notification).

[56] *Id.* at ¶ 230.

[57] *See, e.g.*, *China has Turned Xinjiang into a Police State Like No Other*, ECONOMIST (May 31, 2018), https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other ("A system called the Integrated Joint Operations Platform (IJOP), first revealed by Human Rights Watch, uses machine-learning systems, information from cameras, smartphones, financial and family-planning records and even unusual electricity use to generate lists of suspects for detention. One official WeChat report said that verifying IJOP's lists was one of the main responsibilities of the local security committee. Even without high-tech surveillance, Xinjiang's police state is formidable. With it, it becomes terrifying . . . Islam is a special target.").

[58] *Zakharov v. Russia*, *supra* note 38, at ¶ 230.

[59] *Id.*

[60] 18 U.S.C. § 2703(a) (2018); 18 U.S.C. § 2703(d) (a court order will not be issued without "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."); FED. R. CRIM. P. 41 (a warrant requires probable cause and the identification of the person or property to be searched).

that there are reasonable grounds to believe" information sought is relevant to a crime.[61] An additional layer of independent oversight is provided by OIA's approval of incoming requests and outgoing responses.[62]

If the loss of these protections in new legal instruments is not balanced with alternative protections, much of the world's population may be left vulnerable to arbitrary and abusive data collection practices by domestic law enforcement agencies.

C. *WHAT HAPPENS WHEN THESE LEGAL PROTECTIONS ARE ABSENT*

Far from being a hypothetical concern, both history and contemporary events show that the absence of legal restrictions on government access to data when that data is technically easily obtainable, quickly results in abuses of power, human rights violations, and political control. The Chinese government, for example, uses predictive policing methods, fueled by "big data," to continuously monitor members of an ethnic minority group and deter dissent, ostensibly for national security purposes.[63] Hundreds of thousands of members of this group have been funneled into "concentrated transformation-through-education center[s]."[64]

III. RECENT LEGISLATION AND PROPOSALS

Recently proposed or enacted legal instruments designed to streamline cross-border data access include the U.S. CLOUD Act, the EU's e-Evidence proposal, the Council of Europe's potential Second Additional Protocol to the Budapest Convention, and a proposal for an International Data Access Warrant by the U.N. Special Rapporteur on the right to privacy. Only the CLOUD Act has been enacted.

A. *CLOUD ACT:*

The CLOUD Act enables both the U.S. government and foreign governments to access data controlled by U.S. companies more easily. First, U.S. law enforcement agencies may compel production of data, regardless of where the data are stored.[65] Second, the legislation lifts

---

[61] 18 U.S.C. § 2703(d); *Zakharov v. Russia*, *supra* note 38, at ¶ 260 (discussing the need for reasonable suspicion).

[62] LIN & FIDLER, *supra* note 8, at 2–3.

[63] Human Rights Watch, *China: Big Data Fuels Crackdown in Minority Region* (Feb. 26, 2018), https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region; Human Rights Watch, *China: Police 'Big Data' Systems Violate Privacy, Target Dissent* (Nov. 19, 2017), https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissentl.

[64] Chris Buckley, *China Is Detaining Muslims in Vast Numbers. The Goal: 'Transformation,'* N.Y. TIMES (Sept. 8, 2018), https://www.nytimes.com/2018/09/08/world/asia/china-uighur-muslim-detention-camp.html ("In addition to the mass detentions, the authorities have intensified the use of informers and expanded police surveillance, even installing cameras in some people's homes. Human rights activists and experts say the campaign has traumatized Uighur society, leaving behind fractured communities and families. 'Penetration of everyday life is almost really total now.'").

[65] 18 U.S.C. § 2713 (2018) ("A provider . . . shall comply . . . regardless of whether such communication, record, or other information is located within or outside of the United States.").

restrictions on U.S. company compliance with direct foreign requests made outside of the MLA process, when the foreign government is a party to an executive agreement made pursuant to the CLOUD Act.[66] A state's eligibility for an agreement is determined by the U.S. Attorney General's assessment of the state's legal system.

1. *Speed and Efficiency*

The CLOUD Act is designed to increase the speed and efficiency of cross-border data access for both the U.S. government and selected foreign governments. The legislation eliminates OIA and U.S. judicial approval requirements for states party to executive agreements made pursuant to the Act.[67] It creates reciprocal rights, under which the U.S. government may demand data stored anywhere when controlled by companies under U.S. jurisdiction.[68] This will presumably reduce wait-times from months to days.[69] In addition, this would reduce the OIA's workload, benefitting all states that request data through the U.S. MLA process.

2. *Sovereignty and Extraterritoriality*

While the CLOUD Act prevents jurisdictional conflicts and violations of state sovereignty between the U.S. and parties to executive agreements, it does not necessarily do so for other countries.

The CLOUD Act reduces the risk of violations of state sovereignty between the U.S. and states parties to executive agreements in two ways. First, it creates reciprocal rights of access that remove barriers to direct cooperation between law enforcement agencies in one state and service providers in another.[70] Second, a service provider may file a motion to quash or modify a U.S. demand if compliance would violate the law of a state party to a CLOUD Act agreement.[71] When assessing this motion, a court will engage in a comity analysis, which balances the interests of the U.S. government and foreign governments.[72]

However, the interests of countries not party to an executive agreement are inadequately addressed. Given that data is stored all over the world, it is also likely to be stored in states not party to these agreements.[73] The CLOUD Act does not enable a company to file a motion to modify or quash a U.S. order or warrant due to a conflict of law with a state not party to an executive agreement.[74]

---

[66] 18 U.S.C. § 2703(h)(5) (2018).
[67] 18 U.S.C. § 2523 (2018); 18 U.S.C. § 2703(h)(5).
[68] 18 U.S.C. § 2523(b)(4)(I); 18 U.S.C. § 2713.
[69] *Infra* Part II, Section (A).
[70] 18 U.S.C. § 2523(b)(4)(I).
[71] 18 U.S.C. § 2703(h)(2).
[72] 18 U.S.C. § 2703(h)(3); William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071, 2078 (2015) (defining international comity as "deference to foreign government actors that is not required by international law but is incorporated in domestic law," which is in part a presumption against extraterritoriality).
[73] Reisman, *supra* note 24.
[74] 18 U.S.C. § 2703(h)(2) (stating that motions to quash or modify may be filed where "the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government"); 18 U.S.C. § 2703(h)(1)(A)(i) (defining a qualifying foreign government as one "with which the United States has an executive agreement that has entered into force under section 2523").

3. *Human Rights*

The CLOUD Act promotes human rights protections by conditioning executive agreements on the satisfaction of minimum standards in domestic law and by imposing certain requirements in the terms of agreements and requests made pursuant to these agreements. Though the legislation's long list of conditions and requirements may at first glance seem impressive, upon greater scrutiny, most are meaningless.

i. *Protections in Domestic Law*

The legislation enumerates "factors" the Attorney General must consider when determining whether a potential state party provides sufficiently strong substantive and procedural protections in the context of data collection to qualify for an agreement.[75] Most of these factors are worded ambiguously, effectively making them optional.

The first factor is whether the state is party to the Budapest Convention.[76] Yet this treaty merely reiterates states parties' obligations under general-purpose human rights treaties, and lacks specific protections applicable to cross-border data access.[77]

Second, the state must "demonstrate[] respect for the rule of law and principles of nondiscrimination."[78] Neither the "rule of law" nor the "principle of nondiscrimination" is defined in the CLOUD Act. This is problematic because they are broad terms that can be interpreted in a multitude of ways, some of which are merely formalistic and do not constrain government power in practice.[79]

Third, a state must "adher[e] to applicable international human rights obligations and commitments or demonstrat[e] respect for international universal human rights" with respect to privacy, "the freedom[s] of expression, association, and [] assembly," "prohibitions on arbitrary arrest," "torture, and cruel, inhumane, or degrading" punishment.[80]

Yet these international legal obligations are not completely settled. So, without further clarification, it would be difficult, if not impossible, to make this determination objectively. Applicable treaty language is vague about online privacy and personal data.[81] Jurists and legal scholars are only just beginning to interpret privacy rights for the digital age.[82] Additionally,

---

[75] 18 U.S.C. § 2523(b)(1)(B).

[76] 18 U.S.C. § 2523(b)(1)(B)(i).

[77] Zahid Jamil, *The Budapest Convention: Investigative Powers & Article 15*, COUNCIL EUR. (Aug. 11, 2014), https://rm.coe.int/16803028b2.

[78] 18 U.S.C. § 2523(b)(1)(B)(ii).

[79] *See, e.g.*, BRIAN Z. TAMANAHA, ON THE RULE OF LAW: HISTORY, POLITICS, THEORY, 92–93, 96 (2004) (discussing "rule by law," a concept that guides the Chinese government, as well as the "emptiness of formal legality . . . [which] runs contrary to the long tradition of the rule of law, the historical inspiration of which has been the restraint of tyranny by the sovereign. Such restraint went beyond the idea that the government must enact and abide by laws that take on the proper form of rules, to include the understanding that there were certain things the government or sovereign could not do . . . Formal legality discards this orientation. Consistent with formal legality, the government can do as it wishes, so long as it is able to pursue those desires in terms consistent with (general, clear, certain, and public) legal rules declared in advance.").

[80] 18 U.S.C. § 2523(b)(1)(B)(iii).

[81] *See, e.g.*, International Covenant on Civil and Political Rights art. 17, *opened for signature* Dec. 16, 1966, 92 U.S.T. 908, 999 U.N.T.S. 17; Charter of Fundamental Rights of the European Union, art. 7, 8, 2000 O.J. (C364) 1 (2000).

[82] Most relevant case law and international organization publications postdate 2013. *See, e.g.*, Eur. Ct. H.R., *Guide on Article 8 of the European Convention on Human Rights: Right to Respect*

state practice varies immensely, even between likeminded western democracies, demonstrating that there is insufficient global uniformity to establish customary law.[83]

Moreover, the phrase "adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights" implies that a state *could fail* to satisfy its legal obligations, but nonetheless be certified as a result of an empty gesture.[84]

The remaining factors are only somewhat more concrete. A potential state party must have "clear legal mandates and procedures" authorizing law enforcement data collection, as well as "sufficient" accountability mechanisms and an "appropriate" amount of transparency for this activity.[85] While it is important to determine that a legal basis for this activity exists, the legislation says nothing about the acceptable amount of discretion these mandates and procedures afford foreign law enforcement agencies. What kind of oversight is "sufficient"? What level of transparency is "appropriate"?

Finally, a potential state party must "demonstrate a commitment" to promote and protect Internet openness and the free flow of information.[86] Presumably this provision is intended to discourage data localization, one of the perceived benefits of the legislation, but this language does not prohibit the practice outright.[87]

ii. *Terms of the Agreements*

The CLOUD Act states that an agreement made pursuant to the legislation "shall not create any obligation that providers be capable of decryption data or limitation that prevents providers from decrypting data."[88] Mandated decryption capabilities, or encryption backdoors,

---

for Private and Family Life, Home and Correspondence 92–97 (Aug. 31, 2018), https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf; Joseph A. Cannataci (U.N. Special Rapporteur on the right to privacy), Report of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/HRC/31/64 (Nov. 24, 2016) [hereinafter U.N. Doc. A/HRC/31/64]; Frank La Rue (U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013).

[83] *Compare* Ieuan Jolly et. al., *Data Protection in the United States: Overview*, THOMSON REUTERS PRAC. L. (July 1, 2017), https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1, *with* European Commission, *Data Protection in the EU* (May 6, 2016), https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

[84] 18 U.S.C. § 2523(b)(1)(B)(iii). Empty gestures in international human rights law abound. *See, e.g.*, Declarations, Reservations, Objections and Notifications of Withdrawal of Reservations Relating to the Convention on the Elimination of All Forms of Discrimination against Women, U.N. Doc. CEDAW/SP/2006/2 (Apr. 10, 2006) (enumerating the states parties to CEDAW that have made reservations to Article 2, which effectively nullifies all other CEDAW obligations); International Law Association, International Law Association Report on the Treaty System (1996), http://www.bayefsky.com/reform/ila.php ("For a great many states ratification has become an end in itself, a means to easy accolades for empty gestures . . . [R]atification by human rights adversaries is purchased at a price, namely, diminished obligations, lax supervision, and few adverse consequences from non-compliance.").

[85] 18 U.S.C. §§ 2523(b)(1)(B)(iv)–(v).

[86] 18 U.S.C. § 2523(b)(1)(B)(vi).

[87] *See, e.g.*, Andrew K. Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018), https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems; *contra* Consolidated Appropriations Act of 2018, ch. 119, sec, 105, § 2253(b)(3), Pub. L. No. 115-141, 132 Stat. 348 (2018) (the ambiguous language of the CLOUD Act with the specific language of the draft legal instrument).

[88] 18 U.S.C. § 2523(b)(3).

threaten human rights; in particular the right to hold an opinion, access to information, and freedom of expression.[89] While this language limits one avenue for the creation of encryption backdoors, it wastes an opportunity to prohibit them outright.

iii. *Requirements for Individual Orders*

Requirements for individual orders are designed to limit government discretion, and include purpose limitation, targeting requirements, and rules for sharing and oversight.

a. *Purpose Limitation*

The CLOUD Act limits the purposes for which orders can be sent by foreign governments to "serious crime[s], including terrorism," which may not include infringements on the freedom of speech.[90] Yet the term "serious crime" is undefined, and absent further clarification may be interpreted too liberally.[91]

b. *Proportionality*

The most concrete and stringent legal protections replicate existing U.S. judicial standards. The subject of a data request must be described by "a specific person, account, address, or personal device, or any other specific identifier."[92] Additionally, a request must include "a reasonable justification based on articulable and credible facts, particularity, legality, and the severity regarding the conduct under investigation."[93] These requirements mirror emerging human rights standards, according to which surveillance is permissible only where reasonable and individualized suspicion exists.[94] This narrow targeting helps to prevent disproportionate, indiscriminate data collection.[95]

c. *Safeguards for Sharing*

Importantly, the legislation limits intergovernmental sharing practices that allow governments to circumvent domestic legal protections. First, an individual order cannot be served for the purpose of providing data to the U.S. government or a third country's government.[96] Second, the foreign government "may not" share content with the U.S. government, unless it

---

[89] *See generally* David Kaye (U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/29/32 (May 22, 2015).

[90] 18 U.S.C. § 2523(b)(4)(D)(i); 18 U.S.C. § 2523(b)(4)(E).

[91] *See, e.g.*, Rebecca Hill, *UK.gov Agrees to Narrow 'Serious Crime' Definition for Slurping Comms Data*, REGISTER (July 11, 2018), https://www.theregister.co.uk/2018/07/11/ukgov_agrees_to_narrow_serious_crime_definition_for_sucking_up_comms_data/ (describing how the U.K. government recently increased the minimum imprisonment threshold for a serious crime from six months—which encompasses minor crimes, such as shoplifting—to twelve months, for the purposes of surveillance authorization).

[92] 18 U.S.C. § 2523(b)(4)(D)(ii).

[93] 18 U.S.C. § 2523(b)(4)(D)(iv).

[94] *See Case of Szabó and Vissy*, *supra* note 50, at ¶ 71.

[95] *See e.g.*, *id.*

[96] 18 U.S.C. § 2523(b)(4)(C).

relates to a severe offense, such as terrorism or "significant violent crime."[97] If the U.S. government does receive this information, it must apply minimization procedures derived from the Foreign Intelligence Surveillance Act.[98] These rules partially address the loopholes created by arrangements, such as "Five Eyes" intelligence sharing, in which the U.S. and several partner states reciprocally share information obtained through foreign intelligence operations, which allows each state to systematically circumvent stronger domestic legal safeguards on data collection.[99]

However, these provisions leave open the possibility that a state party could collect large amounts of information on behalf of other countries and share it voluntarily with the implicit understanding that this will be reciprocated. Only the sharing of content with U.S. authorities is restricted, and there is no restriction on sharing information with third countries in the legislation.[100] Yet, as others have discussed in depth, metadata, including subscriber information, is just as revealing content.[101] In practice, these rules will do little to prevent "Five Eyes"-style data sharing arrangements.

iv. *Oversight*

a. *Domestic Oversight*

The legislation requires some form of domestic independent oversight in which each order is reviewable.[102] Yet it provides no additional criteria. The language—"review or oversight" by the judiciary "or other independent authority prior to, or in proceedings regarding, enforcement of the order"—could encompass anything from prior merits-based judicial approval to a merely nominally independent review body that acts as a rubber stamp.[103] If no provisions require meaningful oversight or approval by the judicial or legislative branch, the executive branches could be left to police itself, increasing the risk of abuse.[104]

b. *U.S. Oversight*

Some degree of U.S. oversight is envisioned, though—once again—the imprecise wording could produce anything from systematic oversight to spotty rubber-stamping. The U.S. government may "render the agreement inapplicable" for requests that do not meet the agreement's requirements.[105] In other words, if a foreign request is insufficiently

---

[97] 18 U.S.C. § 2523(b)(4)(H).

[98] 18 U.S.C. § 2523(b)(4)(G)–(H).

[99] *See, e.g.*, Alex Sinha, *British Spying is Our Problem, Too,* AM. C.L. UNION BLOG (Nov. 10, 2014), https://www.aclu.org/blog/national-security/secrecy/british-spying-our-problem-too?redirect=blog/national-security/british-spying-our-problem-too ("The United States has extensive intelligence-sharing arrangements with key allies like the U.K., and through them has access to information that it can't legally collect on its own. Sharing flows both ways, so the U.K. also has unfettered access to much 'raw' or unfiltered U.S. surveillance data.").

[100] 18 U.S.C. § 2523(b)(4)(H).

[101] *See, e.g.*, U.N. Doc. A/HRC/34/60, *supra* note 50, at ¶ 25 (arguing that metadata "are at least as revealing of a person's individual activity as the actual content of a conversation").

[102] 18 U.S.C. § 2523(b)(4)(D)(v).

[103] *Id.*; 18 U.S.C §§ 1804–05 (2010) (describing the perfunctory approval process for surveillance under section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008).

[104] *See, e.g.*, *Case of Szabó and Vissy*, *supra* note 50, at ¶¶ 75, 77.

[105] 18 U.S.C. § 2523(b)(4)(K).

targeted, or the U.S. government does not consider the relevant offense serious, then—for that particular request—the state party would be forced to obtain the information through the normal MLA process or some other method. It is unclear how an improperly invoked order would be detected be the U.S. government, as these agreements would be designed to largely eliminate U.S. government involvement, and the CLOUD Act provides only limited grounds for a company to challenge a foreign request.[106]

Additionally, the state party must agree to "periodic review of compliance" by the U.S. government.[107] The period between reviews is not specified. Would it be monthly, yearly, or perhaps every five years? Would it be effective, enabling American reviewers to access all relevant documents and act to stop abuses?[108]

Outside of the executive branch, only a joint resolution by Congress can block an executive agreement, if it is insufficiently protective of human rights.[109] No judicial challenges are permitted for the certification of a state.[110]

v. *Political Considerations*

Given the flexibility of this language, whether it adequately protects human rights depends almost entirely on how permissively it is interpreted by the Attorney General. Considering the current Attorney General's record on human rights issues, and his apparent lack of legal expertise in online privacy and data protection issues, this does not inspire confidence.[111]

B. *E-EVIDENCE PROPOSAL*

Legislation proposed by the European Commission would permit a judicial or investigative authority to compel the production of electronic evidence for criminal investigations from service provider representatives in the EU, regardless of where the data is stored. The e-Evidence proposal includes a draft directive that would require any service provider "offering services" in the EU to provide a legal representative physically located in the EU to receive data production and preservation orders.[112] These orders, called the European Production Order and the European Preservation Order, would be issued pursuant to the second half of the proposal, a draft regulation.[113] Upon receipt, the representative would be required to preserve or produce sought-after electronic evidence in the service

---

[106] 18 U.S.C. § 2703(h)(2) (2018).

[107] 18 U.S.C. § 2523(b)(4)(J).

[108] *See Zakharov v. Russia*, *supra* note 38, at ¶¶ 281, 282 (discussing elements of oversight effectiveness).

[109] 18 U.S.C. § 2523(d)(4).

[110] 18 U.S.C. § 2523(c).

[111] *See, e.g.*, *Jeff Sessions Issues Directive Undercutting LGBT Protections*, GUARDIAN (Oct. 6, 2017), https://www.theguardian.com/us-news/2017/oct/06/jeff-sessions-issues-directive-undercutting-lgbtq-protections; Vann R. Newkirk II, *The End of Civil Rights*, ATLANTIC (June 18, 2018), https://www.theatlantic.com/politics/archive/2018/06/sessions/563006/.

[112] *Draft Directive*, *supra* note 2, at art. 2(1)–(3), 3 (The definition of "offering services" encompasses major U.S. tech companies, as they "enable[e] legal or natural persons in a Member State to use the services" and "hav[e] a substantial connection to the Member State.").

[113] *Id.* at 5 n.12.

provider's control.[114] Like the CLOUD Act, by rendering the location of data irrelevant, these orders would allow law enforcement authorities in member states to circumvent existing MLAT proceedings.

1. *Speed and Efficiency*

Generally, a company will have a ten-day time limit for compliance.[115] The time limit is reduced to six hours in emergency cases.[116] This is, of course, a dramatically shorter period of time than the months-long wait time member states often face when seeking data through the MLA process.[117]

2. *Sovereignty and Extraterritoriality*

The draft regulation envisions procedures similar to a CLOUD Act comity analysis for potential conflicts of law. If a service provider fears that compliance with a production order will violate the law of a third country, meaning a country outside of the EU, it can send a reasoned objection to the law enforcement agency that issued the order.[118] The agency must then request a review by a court in its state if it wishes to pursue the order.[119] That court must determine whether the third country's law prohibits disclosure.[120] If it finds no conflict, it will order the company to comply.[121] If the court identifies a conflict, and the relevant area of law concerns fundamental rights, national security, or defense, it will leave the decision with the "central authorities" of the affected third country.[122] If the conflict relates to a different area of law, the court in the member state will make the decision alone, according to what is more-or-less a comity analysis, while also taking into account the interests of the company.[123]

Like the U.S. comity analysis, this process would greatly reduce the chance that a third country's territorial sovereignty would be violated, but would not be absolutely preclusive. When evaluating a potential conflict of law arising from something other than fundamental rights, national security, or defense, a member state court would consider "the interest protected by the relevant law of the third country" as one of several factors, and the physical presence of the data in the third state would not be an outright bar to enforcement of the production order.[124]

3. *Human Rights*

The EU's broader legal context—including both EU law and the overlapping European Convention on Human Rights—combined with

---

[114] *Draft Regulation*, *supra* note 2, at art. 9, 10.
[115] *Id.* at art. 9(1).
[116] *Id.* at art. 9(2).
[117] *Infra* Part II, Section (A).
[118] *Draft Regulation*, *supra* note 2, at art. 15, 16.
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.* at art.15(5)–(7).
[123] *Id.* at art.16(5)–(6).
[124] *Id.* at art. 16(5).

requirements in the draft regulation, could render the loss of U.S. procedural protections largely irrelevant.

The EU Charter of Fundamental Rights guarantees the right to privacy and personal data protection.[125] These rights are further clarified in case law from the Court of Justice of the European Union (CJEU), which, among other things, prohibits indiscriminate data collection by governments, and mirrors the "necessary and proportionate" framework found in international legal materials.[126] More specific legislation constrains law enforcement data collection and other surveillance methods.[127] Additionally, all EU member states are party to the European Court of Human Rights (ECHR), which provides similar protections.[128]

The draft regulation specifies its own legal protections. Similar to the U.S. MLA process, it requires prior or subsequent judicial validation for access to content. Unlike U.S. law, it would further require judicial involvement for access to "transactional data," a form of non-content data.[129] Orders would be conditioned upon necessity and proportionality.[130] Additionally, member states would provide an "effective" judicial remedy for people whose data were obtained using a production order.[131] Importantly, both suspects and non-suspects would have access to this remedy.[132] An individual would have the opportunity to challenge the necessity, proportionality, or legality of the order.[133]

Nevertheless, domestic practices can, at least in the short term, undermine regional human rights legal protections.[134] This highlights the

---

[125] Charter of Fundamental Rights of the European Union, art. 7, 8(1), 2000 O.J. (C364) 1 (2000) ("Everyone has the right to respect for his or her private and family life, home and communications . . . Everyone has the right to the protection of personal data concerning him or her.").

[126] Joined cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen, Sec'y of State for Home Dep't v. Watson, 2016 EUR-Lex CELEX LEXIS 970, at ¶¶ 94–96, 103 (Dec. 21, 2016); Case C-362/14. Schrems v. Data Protection Commissioner, Judgment of the Court (Grand Chamber) (E.C.J. 2015) ("[L]egislation permitting the public authorities to have access on a generalised [sic] basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter . . . Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter."); *see also* Joined cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, at 45–54, Judgment of the Court (Grand Chamber) (E.C.J. 2014) ("Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised [sic] by the Union or the need to protect the rights and freedoms of others.").

[127] *See, e.g.*, Council Directive 2016/680, art. 4–11, 53–54, 2016 O.J. (L 119) 89 (EU); Council Regulation 2016/679, art. 48, 2016 O.J. (L 119) 1 (EU).

[128] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, *opened for signature* Nov. 4, 1950, 213 U.N.T.S. 221; *see also, e.g.*, *Zakharov v. Russia*, *supra* note 38, at ¶ 231; *Case of Szabó & Vissy*, *supra* note 50.

[129] *Draft Regulation*, *supra* note 2, at art. 4(2).

[130] *Id.* at art. 5.

[131] *Id.* at art. 17(3) ("Such right to an effective remedy shall be exercised before a court in the issuing State in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality.").

[132] *Id.* at art. 17(1)–(2).

[133] *Id.* at art. 17(3).

[134] *See, e.g.*, *Privacy International, Liberty, and Open Rights Group Joined Other Organisations Across the EU to File Complaints Over Member States' Non-Compliance with Mass Surveillance Rulings*, PRIVACY INT'L, (June 25, 2018),

practical value of an external check on potential abuses of domestic law enforcement powers.

Therefore, despite the robust legal framework provided by the EU and ECHR, the loss of U.S. protections could leave the citizens of at least some EU member states subject to indiscriminate data collection by domestic law enforcement.

C. *ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION*

The Council of Europe's Cybercrime Convention Committee is currently drafting a Second Additional Protocol to the Budapest Convention, with the intention of streamlining access to cross-border electronic evidence.[135] The Budapest Convention requires states parties, which include the U.S. and other non-Council of Europe countries, to both cooperate in MLA requests and maintain certain capabilities for collecting electronic evidence to facilitate this process.[136] The protocol would address contemporary challenges associated with "cloud-based" evidence, which can be stored in different jurisdictions.[137]

Although the final form of the proposal has not yet been published, some details about the drafters' intentions appear in preparatory documents. First, the protocol will likely require state parties to permit service providers in their jurisdictions to disclose subscriber information to law enforcement authorities in other state parties "voluntarily," meaning without a domestic warrant obtained through an MLA process.[138] This would partially replicate the exception in the ECPA that permits U.S. service providers to comply with direct requests for non-content data from foreign governments.[139] Second, it will likely create international production and preservation orders, mirroring the e-Evidence proposal.[140] Third, it will possibly contain additional human rights safeguards to accompany these newly created powers. Fourth, the protocol will likely clarify the restrictions on unilateral measures issued to circumvent the MLA process.[141]

1. *Speed and Efficiency*

Hypothetically, voluntary disclosure regimes and mandatory production orders would reduce waiting periods for access to cross-border data. Given that subscriber data is the most sought type of data in law enforcement investigations, a voluntary disclosure scheme would greatly

---

https://privacyinternational.org/press-release/2119/privacy-international-liberty-and-open-rights-group-joined-other-organisations [hereinafter *Privacy International*].

[135] *Terms of Reference*, *supra* note 2; *see also Discussion Guide for Consultations with Civil Society, Data Protection Authorities and Industry*, CYBERCRIME CONVENTION COMMITTEE, (May 21, 2018), https://rm.coe.int/t-cy-2018-16-pdp-consultations-paper/16808add27 [hereinafter *Discussion Guide*]. For those unfamiliar with the difference between the EU and Council of Europe institutions, see *Do Not Get Confused*, COUNCIL EUROPE, https://www.coe.int/en/web/about-us/do-not-get-confused (last accessed Apr. 20, 2019).

[136] Budapest Convention, *supra* note 2, at art. 14, 29–34.

[137] *Terms of Reference*, *supra* note 2, at 3.

[138] Budapest Convention, *supra* note 2, at art. 18 (defining subscriber information as non-content information pertaining to a user's identity, postal or geographic address, telephone or other access number, and billing or payment information); *Discussion Guide*, *supra* note 135, at 5–6.

[139] *Discussion Guide*, *supra* note 135, at 5–6.

[140] *Id.* at 7.

[141] *Terms of Reference*, *supra* note 2, at 34; *Discussion Guide*, *supra* note 135, at 3.

help to alleviate the overall burden of the existing MLA regime.[142] Currently, most state parties to the Convention do not permit this kind of direct cooperation with foreign law enforcement requests.[143]

Additionally, an international production order modeled after the European Production Order would presumably reduce waiting periods, as it would likely eliminate foreign MLA proceedings for law enforcement agencies.[144] A mandatory production order, like the proposed European Production Order, would prevent situations in which a service provider chooses not to comply with a discretionary request.[145]

2. *Sovereignty and Extraterritoriality*

By coupling mandatory production orders with voluntary disclosure regimes, the Protocol would reduce the likelihood of friction between states concerning jurisdiction over data. Assuming the Protocol would require reciprocal rights for state parties—this prior consent would prevent violations of state sovereignty between state parties.[146] Furthermore, the voluntary disclosure scheme would help to prevent conflicts from arising by preventing the use of coercive legal methods or the need for approval by foreign governments.[147]

3. *Human Rights*

Few details have been provided about the Protocol's potential human rights protections. However, given how little print space has been devoted to the topic thus far, it may wind up being an afterthought.[148] This would not be surprising, given that the same could be said about the Budapest Convention, which merely reiterates governments' obligations under general-purpose human rights treaties.[149]

This presents a problem because there is substantial variation in the domestic legal protections afforded by parties to the Budapest Convention to people whose data are sought in law enforcement investigations. While most parties are members of both the Council of Europe and the EU, whose legal frameworks, at least hypothetically, provide robust baseline human rights protections, some state parties provide far weaker or qualitatively different protections. For example, recently enacted data protection legislation in Turkey provides few checks on government abuse of data collection powers.[150]

Nationals of these countries would suffer a loss of U.S. procedural protections for content and easier access to subscriber information in other countries. Mandatory production orders would deprive non-U.S. persons the external check currently provided by the U.S. MLA process on the

---

[142] *T-CY Assessment Report*, *supra* note 4, at 123.

[143] *Discussion Guide*, *supra* note 135, at 5.

[144] *See infra* Part IV, Section (B)(1); *Discussion Guide*, *supra* note 135, at 7.

[145] *See, e.g.*, *Impact Assessment*, *supra* note 7, at 15–16 (demonstrating that less than half of direct requests sent by EU member States to (mainly U.S.) service providers are fulfilled).

[146] *See infra* Part II, Section (C).

[147] *Id.*

[148] *See generally Terms of Reference*, *supra* note 2; *Discussion Guide*, *supra* note 135.

[149] Budapest Convention, *supra* note 2, at art. 15(1).

[150] Craig Shaw & Zeynep Sentek, *'Citizens Will Be Stripped Naked' by Turkey's Data Law*, COMPUTER WKLY. (Apr. 5, 2016), https://www.computerweekly.com/news/450280254/Citizens-will-be-stripped-naked-by-Turkeys-data-law.

abuse of data collection powers by domestic law enforcement agencies; at least with regard to content. Additionally, while the U.S. already permits companies to voluntarily disclose subscriber information, this is problematic, and the expansion of this practice would be even more so. Ready availability of subscriber information undermines online anonymity, which is crucial for the protection of human rights in the digital age.[151]

D. *INTERNATIONAL DATA ACCESS WARRANT*

These differences in domestic human rights protections would be rendered largely irrelevant in the draft legal instrument under consideration by the U.N. Special Rapporteur on the right to privacy.[152] As a potential international treaty, it would impose common standards and rules pertaining to cross-border data access derived from international human rights law and would also transfer authorization power from domestic authorities to an international body.

As it now stands, the draft legal instrument would create an alternative to the MLA process through the creation of an international judicial body empowered to issue International Data Access Warrants.[153] A domestic law enforcement agency or investigator could send an application directly to this judicial body, which could then issue a warrant to a service provider located in any other state party.[154]

1. *Speed and Efficiency*

Though no maximum response time is specified, the scheme envisioned in the draft legal instrument would increase the speed and efficiency of the data access process through remote deliberations, adequate resourcing, twenty-four hour scheduling, and more generally, providing a streamlined procedure.[155] State parties would be required to provide "adequate resources for the efficient working" of the bodies created by the instrument, which would help to prevent OIA-style backlogs.[156] Wherever possible, proceedings would be carried out online.[157] Empirical evidence shows that online dispute resolution tools, including remote video testimony, reduce the length and cost of judicial proceedings.[158] This "one-stop shop" would eliminate the need for lengthy and complex approval processes in U.S. courts and central authorities.[159]

---

[151] *See generally* Kaye, *supra* note 89.

[152] *Draft Legal Instrument*, *supra* note 2; *Report of the Special Rapporteur on the Right to Privacy* at ¶¶ 114, 127, U.N. Doc. A/HRC/37/62 (Feb. 28, 2018) [hereinafter U.N. Doc. A/HRC/37/62].

[153] *Draft Legal Instrument*, *supra* note 2, at art. 15.

[154] *Id.* at art. 4(1)(j), 15(2)(b)(ii).

[155] *Id.* at art. 15(3)–(5), art. 15 cmt. 1310–15 ("The creation of such a mechanism would, if the IDAA is properly resourced and staffed, cut down waiting times for transfer of personal data required by law enforcement, prosecutors and intelligence services by weeks and often by an average of up to eleven months. With panels of judges working world-wide in a secure on-line manner, on a rota 24/7, urgent requests for access to personal data, whether in real-time or historical, for legitimate surveillance purposes could be handled quickly and efficiently.").

[156] *Id.* at art. 15(4)–(5) (any state failing to make its required contributions would be suspended).

[157] *Id.* at art. 15(3)(a).

[158] *Id.* at art. 15(4).

[159] *Id.* at art 15 cmt. 1297.

2. *Sovereignty and Extraterritoriality*

At least among parties to the not-yet-proposed instrument, this design would prevent violations of state sovereignty and reduce the risk of international discord. Service providers in state parties would be required to comply with International Data Access Warrants and could not justify noncompliance on the basis of jurisdiction or territoriality.[160] A state could not circumvent the international warrant process via unilateral measures, absent another form of prior consent from the affected state.[161]

Importantly, this draft instrument could take the form of an international treaty, potentially open to all U.N. member states.[162] The resulting universal or near-universal consent could effectively render uncertainty about jurisdiction irrelevant.

3. *Human Rights*

Unsurprisingly, the draft legal instrument features a robust human rights framework, consisting of multilayered independent oversight, including prior judicial authorization, and stringent domestic legal protections.

i. *Oversight*

a. *Prior Judicial Authorization*

An international judicial body established by the draft legal instrument would approve or reject applications from domestic law enforcement agencies for International Data Access Warrants.[163] This body would be comprised of a lower-level body called the International Data Access Commission and an appellate-level body called the International Data Access Tribunal.[164] Each application for data access would be assessed by a panel of three judges in the Commission, and, if appealed, by five judges in the Tribunal.[165]

The independence of decision-making would be guaranteed not only by the involvement of judges, but also by the insulation of judges from domestic political pressure. Though judges would be nominated by state parties, they would be remunerated by an independent body established by the draft legal instrument.[166] Decisions would be based on simple majority votes by panels randomly selected through automation, with only one seat reserved for a judge nominated by the applicant state.[167] It would be highly unlikely that one state's executive branch could effectively influence the outcome of a decision through political pressure.[168]

---

[160] *Id.* at art. 4(1)(j).
[161] *Id.* at art. 4(4)(a).
[162] *See, e.g.*, U.N. Doc. A/HRC/37/62, *supra* note 152, at ¶ 127.
[163] *Draft Legal Instrument*, *supra* note 2, at art. 15(2)(b), (d).
[164] *Id.*
[165] *Id.*
[166] *Id.* at art. 15(2)(b)(i), 15(2)(d)(i), 15(4)(a).
[167] *Id.* at art. 15(2)(b)(iii).
[168] In fact, interference with the workings of the commission would result in suspension from the international warrant system. *See id.* at art. 15(6).

b. *Systematic Oversight*

More general oversight would be carried out by two committees. A committee of human rights legal experts called the Committee of Human Rights Defenders would produce an annual report, including the number of cases monitored, difficulties encountered in the course of this work, and recommendations for best practices.[169] A second consultative committee would monitor all procedures undertaken pursuant to the legal instrument and make recommendations about the interpretation of, and potential amendments to, the legal instrument.[170]

ii. *Adversarial Component*

In each warrant application process, a Human Rights Defender would be randomly assigned to monitor the process, and if appropriate, advocate on behalf of the subject.[171] The Human Rights Defender would "have the right of audience and to present arguments . . . where it is felt that [the] surveillance requested is unnecessary, disproportionate or in any way breaches [the subject's] fundamental human rights."[172]

iii. *Domestic Legal Requirements*

Eligibility for ratification of the draft legal instrument would, in part, be conditioned upon the adoption of stringent human rights protections in domestic law for domestic surveillance.[173] Among these requirements is multilayered oversight that includes independent prior authorization, a sufficiently detailed and publicly accessible legal basis for surveillance, requirements for necessity, proportionality, and reasonable suspicion, and a remedy.[174]

E. *COMPARING THE PROPOSALS*

Only the draft legal instrument for the International Data Access Warrant adequately addresses challenges related to speed, jurisdiction, and human rights.

1. *Speed and Efficiency*

By eliminating the need for MLA procedures, the CLOUD Act, e-Evidence proposal, Budapest Convention, and the draft legal instrument for an International Data Access Warrant would increase the speed and efficiency of cross-border data access. The elimination of MLA proceedings, including domestic and foreign central authority scrutiny, as well as judicial approval for incoming U.S. requests, would dramatically simplify the process. Each legal instrument would provide an alternative

---

[169] *Id.* at art. 15(2)(c).

[170] *Id.* at art. 15(2)(a) (the committee is tentatively called the "Surveillance Legal Instrument Consultative Committee").

[171] *Id.* at art. 15(2)(c)(v)(1), 15(2)(c)(iii), 15(2)(c)(v)(2).

[172] *Id.* at art. 15(2)(c)(v)(2); *id.* at art. 2(1) (Surveillance is defined in the instrument to include data collection.).

[173] *Id.* at art. 3–13.

[174] *Id.* at art. 3.

to, or simply eliminate, foreign MLA requirements.[175] These streamlined procedures would likely shave months off of response times, at least in the U.S.[176] The e-Evidence proposal envisions a response time of ten days or less in non-emergency situations, in contrast to its current wait-time of one to six months.[177]

Additionally, the overall reduction of OIA's caseload would presumably shrink its backlog and reduce wait-times for states not party to, or beneficiaries of, these instruments. Caseloads in other states could be reduced further by the voluntary disclosure regime for subscriber data envisioned in the forthcoming protocol to the Budapest Convention.[178]

2. *Sovereignty and Extraterritoriality*

To varying degrees, these legal instruments would reduce the risk of violations of state sovereignty and conflicts of law through the removal of blocking provisions and application of comity analysis.

Executive agreements made pursuant to the CLOUD Act would eliminate "blocking" provisions in the U.S. and parties to these agreements, allowing service providers to respond directly to foreign data requests.[179] The uncompleted Second Additional Protocol to the Budapest Convention would adopt a similar scheme for subscriber data.[180]

Additionally, pursuant to the CLOUD Act, a service provider may challenge a U.S. request if it would potentially create a conflict of law with a party to an executive agreement. In assessing the motion, the court would perform a comity analysis, which includes a presumption against extraterritoriality.[181] The e-Evidence proposal contains a more inclusive mechanism to prevent conflicts of law. If a request potentially creates a conflict of law with any country (not only pre-approved countries), a service provider may challenge the request.[182] Additionally, the government of the affected country would in certain circumstances have the opportunity to deny the request.[183]

While reducing the chance of international discord, the CLOUD Act and e-Evidence proposal would not entirely prevent violations of state sovereignty through unapproved cross-border data access. Given service providers' dynamic and global data storage practices, situations will inevitably arise in which a provider is ordered to produce data stored in a country that has not given consent through a CLOUD Act agreement or other legal instrument.[184] The CLOUD Act's comity analysis only follows from potential conflicts with parties to agreements, and the e-Evidence

---

[175] *Id.* at art. 15; 18 U.S.C. § 2523 (2018); 18 U.S.C. § 2703(h)(5) (1988); *Draft Regulation*, *supra* note 2, at art. 1.

[176] *See infra* Part II, Section (A).

[177] *Draft Regulation*, *supra* note 2, art. 9(1).

[178] *Terms of Reference*, *supra* note 2, at 3.

[179] 18 U.S.C. § 2703(h)(5).

[180] *Terms of Reference*, *supra* note 2, at 3.

[181] 18 U.S.C. § 2703(h)(2); Dodge, *supra* note 72.

[182] *Draft Regulation*, *supra* note 2, at art. 15–16.

[183] *Id.* at art. 15(6).

[184] Reisman, *supra* note 24.

proposal's conflict mechanism—while generous—does not entirely prevent unapproved access.[185]

More troubling is the inevitability that this approach—a government empowering itself to compel data stored in any country through domestic (or EU) law—will be copied by governments likely to abuse that power. This could give rise to "a potentially dangerous and uncoordinated race to the bottom."[186]

It follows that violations of state sovereignty and conflicts of law would occur less frequently where an inclusive multilateral agreement creates prior consent for direct access by foreign governments, as well as a degree of legal uniformity among state parties. This is what the draft legal instrument for an International Data Access Warrant would accomplish. This legal instrument would impose a set of stringent minimum human rights standards in government surveillance, and state parties would agree to require service providers in their jurisdiction to comply with International Data Access Warrants.[187]

3. *Human Rights*

While both the CLOUD Act and e-Evidence proposal leave domestic and regional protections for U.S. and EU citizens more-or-less intact, both are likely to directly or indirectly result in weaker protections for people in other jurisdictions. In contrast, the draft International Data Access Warrant instrument has the potential to increase the strength of legal protections worldwide.

As discussed above, executive agreements made pursuant to the CLOUD Act contain few concrete legal protections for non-U.S. persons whose data are obtained from U.S. companies.[188] Rather than using the legislation as an opportunity to impose higher standards, the authors appear to simply have treated foreign human rights protections as a nuisance.

Additionally, both the CLOUD Act and e-Evidence proposal empower U.S. and EU member state law enforcement agencies to demand data located anywhere in the world outside of the MLA process. This sets a bad precedent for states with weak protections in the context of government data collection.[189] Governments in these states will likely copy the U.S. and EU approach, demanding data outside of the MLA process—thereby depriving their nationals of the protections afforded by foreign law and increasing the likelihood of human rights violations.[190]

In contrast, the draft proposal for the International Data Access Warrant has the potential to reduce the risk of abuses of data collection

---

[185] 18 U.S.C. § 2703(h)(ii); *Draft Regulation*, *supra* note 2, art. 15–16 (A conflict of law unrelated to fundamental rights, national security, or defense prompts a balancing test, rather than an absolute bar to data production.).

[186] Katitza Rodriguez, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom*, ELECTRONIC FRONTIER FOUND. (Apr. 9, 2018), https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom.

[187] *See infra* Part IV, Section (D).

[188] *See infra* Part IV, Section (A)(3).

[189] Rodriguez, *supra* note 186.

[190] *Id.* Compare this with the Russian government's duplication of Germany's Network Enforcement Act ("fake news law"), which is more ominous in the context of Russia's weak human rights legal protections. *See, e.g.*, *Russian Bill is Copy-and-Paste of Germany's Hate Speech Law*, REPS. WITHOUT BORDERS (July 19, 2017), https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law.

powers, while increasing the strength of related human rights protections around the world. Unlike the CLOUD Act's slippery language, the myriad of human rights protections upon which ratification is conditioned are sufficiently specific and concrete to ensure that they are not interpreted in ways that render them meaningless.[191] Additionally, the international judicial mechanism does not set a bad precedent for governments wishing to increase the scope of data collection powers for unsavory purposes. In fact, it requires states to relinquish power by narrowing the scope of permissible domestic and cross-border data collection.

4. *Summary*

The draft proposal for the International Data Access Warrant is the only instrument that would increase the speed and efficiency of cross-border data access, have a high likelihood of preventing violations of state sovereignty and conflicts of law, and provide reliably strong human rights protections. From a legal perspective, it is ideal. However, from a political perspective, it is not.

IV. NEGOTIATING THE INTERNATIONAL DATA ACCESS WARRANT PROPOSAL

A. *WHY IT WOULD BE DIFFICULT*

Given the usual challenges associated with the creation of international human rights treaties, and the degree to which states zealously guard their surveillance powers in particular, the draft International Data Access Warrant mechanism could be a hard sell. Yet its strengths merit the work necessary to bring it to fruition. The CLOUD Act and, if enacted, e-Evidence proposal could create breathing room to allow the U.S., EU, and the rest of the international community to put a more sustainable solution in place.

At a first glance, governments may understandably find the draft legal instrument unrealistic. The creation of international human rights instruments has never been an easy task.[192] Negotiations are often long and—given the diversity of political views represented—contentious.[193]

---

[191] *Compare* 18 U.S.C. § 2523(b)(1)(B)(v) (2018) (creating an ambiguous "appropriate transparency" standard), *with Draft Legal Instrument*, *supra* note 2, at art. 4(2)(a)–(b) (enumerating procedures such as "[p]ublicly available, periodic reports allowing for a substantive and comprehensive review of the activities of relevant agencies to other State entities such as the legislative branch and/or the judicial branch" and "[p]ublicly available transparency reports by the State itself in respect to all requests made to corporations and other non-state actors with regard to the provision of personal data including categories, and frequency").

[192] *See, e.g.*, MARY ANN GLENDON, A WORLD MADE NEW: ELEANOR ROOSEVELT AND THE UNIVERSAL DECLARATION OF HUMAN RIGHTS (2001) (describing the negotiation process—in particular the friction between representatives of the then-Soviet Union and Western democracies—that gave rise to the Universal Declaration of Human Rights, and ultimately, the International Covenant on Civil and Political Rights and International Covenant on Economic, Social and Cultural Rights); Elizabeth Sepper, *Confronting the "Sacred and Unchangeable": The Obligation to Modify Cultural Patterns Under the Women's Discrimination Treaty*, 30 U. PA. J. INT'L L. 585, 594 (2008) (describing the protracted and hotly-contested negotiations behind the Convention on the Elimination of All Forms of Discrimination Against Women).

[193] GLENDON, *supra* note 192.

These difficulties would be amplified in the context of a treaty concerning online privacy and surveillance. Whether legitimate or cynical, governments' contemporary preoccupation with terrorism causes them to stubbornly hold onto what are arguably disproportionate and unlawful surveillance powers, and even call for expanded powers, in spite of intensive reform efforts and contrary court decisions.[194] Additionally, MLAT reform is a time-sensitive issue, given OIA's rapidly increasing case burden, as well as the need to prevent the spread of data localization and other problematic unilateral measures.

B. *WHY IT IS WORTHWHILE*

Nevertheless, the draft proposal warrants the effort it would take for the U.S., EU, and other governments to actualize it. It would provide an effective, long-term solution for speedy and lawful cross-border data access that would prevent human rights abuses. It would not trigger a "race to the bottom," in which expansions of domestic power to access cross-border data give rise to more conflicts of law, violations of state sovereignty, and weakened human rights protections worldwide. Human rights protections would be a cornerstone, rather than an afterthought. At a minimum, it would prevent the kinds of excesses and abuses seen in China, with effective limitations on both cross-border data access and purely domestic surveillance activities. Thus, governments should treat the CLOUD Act and e-Evidence proposal as stopgap solutions and follow the Special Rapporteur's recommendation to start empowering their executive branches to "actively explore" the draft legal instrument and similar proposals.[195]

Once committed, governments may find the process easier than expected. Governments worldwide would have a strong incentive to support the proposal, given their urgent need for more rapid access to cross-border data. Civil society would have a strong incentive to support the proposal, as it would satisfyingly address both human rights advocates' concerns about online privacy and data protection and companies' desire to avoid conflicts of law. Increasingly, privacy-conscious publics would likely be receptive to this scheme. The Special Rapporteur expects that the "number of states coalescing around newly-articulated principles and newly created mechanisms could gradually grow to provide critical mass . . . [and that this] time may be sooner than some may wish us to think."[196]

CONCLUSION

That "[t]he natural tendency of Government is toward abuse of power," was noted by a congressional oversight committee in its 1976

---

[194] *See, e.g.*, *Privacy International*, *supra* note 134; Rebecca Hill, *Spies Still Super Upset They Can't Get at Your Encrypted Comms Data*, REGISTER (Aug. 31, 2018), https://www.theregister.co.uk/2018/08/31/five_eyes_2018_meeting_encryption_terrorist_content/; Louise Matsakis, *Congress Renews Warrantless Surveillance – and Makes it Even Worse*, WIRED (Jan. 11, 2018), https://www.wired.com/story/fisa-section-702-renewal-congress/.

[195] U.N. Doc. A/HRC/34/60, *supra* note 50, at ¶ 46(k).

[196] *Id.* at ¶ 46(l).

report about U.S. government surveillance.[197] This is why "[c]lear legal standards and effective oversight and controls are necessary to ensure that domestic intelligence activity does not itself undermine the democratic system it is intended to protect."[198] The European Court of Human Rights came to a similar conclusion two years later, when it noted that a law affording a government unlimited discretion in domestic surveillance created a "danger . . . of undermining or even destroying democracy on the ground of defending it," and therefore, required "adequate and effective guarantees against abuse."[199]

Consequently, the court and U.S. Congress mandated similar independent judicial (or "preferably judicial" in the court's judgment) oversight requirements.[200]

Some argue that the increased volume and importance of electronic evidence in contemporary law enforcement investigations necessitate weaker procedural protections for individuals, because of the burden high standards place on investigators. Yet if one bears in mind the purpose of these protections—preventing the abuse of power—the increased volume and importance of electronic communications in contemporary life, if anything, demands stronger protections. This makes *clear*—as opposed to ambiguous—legal standards and *effective*—as opposed to perfunctory and impotent—oversight and controls are as indispensable today as they were thirty years ago.

For that reason, a legal instrument governing cross-border data access must prioritize human rights protections, rather than carelessly strip them away. The instrument must also accommodate the borderless nature of the Internet to avoid violations of state sovereignty and conflicts of law, while expediting the process. The draft International Data Access Warrant proposal would best accomplish these goals.

---

[197] S. REP. No. 94–755, at 291 (1976).

[198] *Id.* at 20.

[199] *Case of Klass and Others v. Germany (Application no. 5029/71)*, HUDOC ¶¶ 49–50 (1978), http://hudoc.echr.coe.int/eng?i=001-57510.

[200] *Id.* at 55; S. Rep. No. 94–755, *supra* note 197; BARRY E. FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 287–89 (2017) (noting that the Foreign Intelligence Surveillance Act, the creation of which was prompted by the Church Committee report, imposed a warrant requirement for foreign intelligence surveillance targeting U.S. persons).