Richmond Journal of Law & Technology

Volume 22 | Issue 1 Article 2

2015

MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance

Sarah Cortes

MLAT JIU-JITSU AND TOR: MUTUAL LEGAL ASSISTANCE TREATIES IN SURVEILLANCE

Sarah Cortes

Cite as: Sarah Cortes, *MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance*, 22 RICH. J.L. & TECH. 2 (2015), http://jolt.richmond.edu/v22i1/article2.pdf.

I. INTRODUCTION: RISE OF SURVEILLANCE, MLATS, ANONYMITY, MJATS

[1] A corrupt Australian Law Enforcement Agency (LEA) wishes to track the communications of a journalist who has published leaked whistleblowing documents from a confidential source, revealing the Australian LEA's complicity in illegal narcotics activity. The target journalist lives in New York and is a U.S. citizen. She opens her laptop, goes online and fires up Tor Browser.[1] She is communicating with her whistleblowing source in Australia, who faces death if his identity is uncovered. Her communication and network traffic passes through Tor relays in Canada, Finland, and Malaysia before arriving at her source in Australia.[2]

[2] In what we call an "MLAT cartel attack" against online privacy tools, Australia uses treaty relationships with other countries to facilitate surveillance.[3] The communication service providers (CSPs) under their

[1] *See generally Tor Browser*, TOR, https://www.torproject.org/projects/torbrowser.html.en, *archived at* https://perma.cc/FCM7-LMAC (last visited Dec. 2, 2015) (describing and explaining Tor generally, in that it allows you to search the Internet without being tracked).

[2] Tor relays function to "receive traffic on the Tor network and pass it along." *What Is Tor?*, TOR CHALLENGE, http://www.eff.org/torchallenge/what-is-tor.html, *archived at* http://perma.cc/6DKA-SY2B (last visited Oct. 4, 2015).

[3] *See* Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power, and Mass Surveillance in the U.S. and Europe*, 10 ISJLP 481, 483 (2014).

jurisdiction all implemented automated surveillance through unclear legal means. Once surveillance is automated and normalized, it becomes easier to bypass Fourth Amendment protections,[4] skipping meaningful judicial oversight or a show of probable cause—asking forgiveness rather than permission.

[3] The corrupt Australia LEA presses the button, targeting the journalist's network traffic,[5] hoping to find her source. Traffic correlation[6] and timing attacks[7] enable the corrupt Australian LEA to capture the journalist's outgoing message as it travels through the Tor network—and she discovers the identity of her whistleblower in short order. It is the last time the American journalist hears from her source—who has been silenced.

[4] Since Edward Snowden recommended the use of the TorBrowser as one of his top tips for whistleblowers and ordinary people to protect

[4] *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[5] Actually, the IP address of the journalist's home router, to which her laptop is attached.

[6] *See, e.g.*, AARON JOHNSON, CHRIS WACEK, ROB JANSEN, MICAH SHERR & PAUL SYVERSON, USERS GET ROUTED: TRAFFIC CORRELATION ON TOR BY REALISTIC ADVERSARIES, at sec. 3 (20th ACM Conference on Computer and Communications Security, Nov. 2013) [hereinafter CCS 2013], http://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/13-1231-2077.pdf, *archived at* http://perma.cc/V93X-5XW5 (describing how Tor and traffic correlation attacks can work together).

[7] *See, e.g.*, RISHAB NITHYANAND, OLEKSII STAROV, ADVA ZAIR, PHILLIPA GILL & MICHAEL SCHAPIRA, MEASURING AND MITIGATING AS-LEVEL ADVERSARIES AGAINST TOR 1, 14 (Aug. 18, 2015), http://arxiv.org/pdf/1505.05173.pdf, *archived at* http://perma.cc/55MK-Q94T (asserting that there are high rates of susceptibility to traffic correlation and timing attacks for Tor users, correlating to potentially high probability of successful capture).

their privacy and anonymity online,[8] policymakers are becoming aware of Tor's role in protecting identity online. For instance, Snowden leaked a document revealing the NSA project "EgotisticalGiraffe", which had the objective of breaking underlying Tor encryption and privacy protections.[9] In this paper, we document how MLATs can assist in such attacks on Tor.

[5] The documents released by Snowden reveal far greater levels of U.S. and other government surveillance than previously known,[10] including surveillance outside the US and across multiple country borders.[11] This widespread surveillance includes online data and

[8] *See* Brian Fitzgerald, *Snowden at SXSW: Encryption Must Be Stronger*, DIGITS: WALL ST. J. (Mar. 10, 2014, 11:47 AM), http://blogs.wsj.com/digits/2014/03/10/live-video-edward-snowden-at-sxsw/, *archived at* http://perma.cc/K9V4-KZQK (citing a Twitter post by an individual attending the conference).

[9] *See* Peeling Back the Layers of Tor with Egotistical Giraffe, THE GUARDIAN (Oct. 4, 2013, 10:49 AM), http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document, *archived at* http://perma.cc/ZE6B-S6YF; s*ee also* James Ball, Bruce Schneier, & Glenn Greenwald, *NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users*, THE GUARDIAN (Oct. 4, 2013, 10:50 AM), http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption, *archived at* http://perma.cc/CA5Q-4F56; Barton Gellman, Craig Timberg, & Steven Rich, *Secret NSA Documents Show Campaign Against Tor Encrypted Network*, WASH. POST (Oct. 4, 2013), http://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html, *archived at* http://perma.cc/VM4M-ADY3.

[10] *See* Glenn Greenwald, Ewen MacAskill, & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 9, 2013, 9:00 AM), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, *archived at* http://perma.cc/K2ZC-Z94B.

[11] *See* Laura Poitras, Marcel Rosenbach, Michael Sontheimer, & Holger Stark, *A Two-Faced Friendship: Turkey Is 'Partner and Target' for the NSA*, SPIEGEL ONLINE INT'L (Aug. 31, 2014, 12:00 PM), http://www.spiegel.de/international/world/documents-show-nsa-and-gchq-spied-on-partner-turkey-a-989011.html, *archived at* http://perma.cc/8VRA-P3TX.

telecommunications; much of it culled from third-party communication service providers ("CSPs").[12] With the expansion of surveillance came the expansion of U.S. law legalizing surveillance, such as the U.S. Patriot Act.[13] Some contend that much of this surveillance—often referred to by LEAs as lawful intercept ("LI")—is actually *unlawful*.[14]

[6] These changes in government surveillance have resulted in several undesirable circumstances, including government attempts to apply pressure directly on third-party CSPs operating within their borders.[15]

---

[12] *See id.*

[13] *See* U.S. Patriot Act, Pub. L. No. 107-56, § 201, 115 Stat. 272, 278 (2001); Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279, 4282 (1994).

[14] *See* Steve Erlanger, *Fighting Terrorism, French-Style*, N.Y. TIMES (Mar. 30, 2012), http://www.nytimes.com/2012/04/01/sunday-review/the-french-way-of-fighting-homegrown-terrorism.html, *archived at* http://perma.cc/7JJ2-BRU7; Scott M. Fulton, *EU's Reading to Cloud Providers: Stop Sheltering Yourself from US Patriot Act*, READWRITE.COM (Dec. 6, 2011), http://readwrite.com/2011/12/page/eus-reding-to-cloud-providers, *archived at* http://perma.cc/HR9T-B4DA.

[15] *See, e.g.*, Declan McCullagh, *FBI Pressures Internet Providers to Install Surveillance Software*, CNET (Aug. 2, 2013, 12:26 PM), http://www.cnet.com/news/fbi-pressures-internet-providers-to-install-surveillance-software/, *archived at* http://perma.cc/6WA8-3H39; Complaint at paras. 2, 7, 10, 13–14, Jewel v. Nat'l Sec. Agency, No. C 08-04373 (N.D. Cal. Sept. 18, 2008), https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf, *archived at* https://perma.cc/M7M4-PB2M. Jewel was one of the first to challenge the NSA's massive domestic data collection program as "un" lawful interception. *See NSA Spying on Americans: Jewel v. NSA*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/jewel, *archived at* https://perma.cc/77CR-972V (last visited Oct. 1, 2015). The NSA's defense has revolved around assertions under the state secrecy privilege. Gov't Def.'s Reply in Supp. of Mot. to DIsmiss and for Summ. J. at 1, 7, Jewel v. Nat'l Sec. Agency, No. C:08-cv-4373 (N.D. Cal. June 26, 2009), https://www.eff.org/files/filenode/jewel/jewel_gov_reply.pdf, *archived at* https://perma.cc/AZC8-5TXC. So far, the courts have declined to dismiss the case based on state secrets. *See, e.g.*, Order at 2, Jewel v. Nat'l Sec. Agency, No. C 08-04373 (N.D. Cal. July 8, 2013), https://www.eff.org/files/filenode/jewelorder.pdf, *archived at* https://perma.cc/E42U-A6Y7. On March 10, 2014, the court issued a temporary

Coincident with the rise of online government surveillance has been a rise in a little-noticed legal tool—the international Mutual Legal Assistance Treaty (MLAT).[16] Governments control the CSPs, which own or operate IT infrastructure over which network traffic passes.[17] MLATs provide vector for government intelligence agencies (GIAs) to facilitate global surveillance—technically and legally—through exploiting this control.

[7] MLAT expansion facilitates surveillance and erodes civil liberties in three distinct ways. First, specific MLAT provisions explicitly eliminate existing civil liberties. Second, MLATs provide a legal framework for mass cross-border surveillance. Third, MLATs technically facilitate surveillance by controlling CSPs, encouraging technical surveillance automation, and attacking online privacy and anonymity protecting tools. We review recent MLAT circuit court rulings—including *United States v. Getto*, decided by the Second Circuit on September 30, 2014.[18]

---

restraining order halting NSA's destruction of evidence. Order Granting TRO at 1–2, Jewel v. Nat'l Sec. Agency, No. C 08-04373 (N.D. Cal. Mar. 10, 2014), https://www.eff.org/files/2014/03/11/089_order_granting_tro_3.10.14.pdf, *archived at* https://perma.cc/8GM4-CHDM. On June 5, 2014, EFF filed an application for an emergency hearing upon learning that the NSA was continuing to destroy evidence. Plaintiff's Emergency Appl. to Enforce the Court's TRO at 1–2, Jewel v. Nat'l Sec. Agency, No. C:08-cv-4373 (N.D. Cal. June 5, 2014), https://www.eff.org/files/2014/06/05/jewel_emergency_app_enforce_tro.pdf, *archived at* https://perma.cc/NBP2-HVHJ.

[16] For more information, see Sarah Cortes, *Dynamic Triggering: MLATs, Third Parties and ETSI TS 102 677 Automated Surveillance* (Sept. 30, 2014) (unpublished manuscript) (on file with author) [hereinafter *Dynamic Triggering*].

[17] *Id.*

[18] *See generally* United States v. Getto (*Getto II*) 586 Fed. App'x 11 (2d Cir. 2014) (finding Getto was guilty of conspiracy to commit wire fraud and mail fraud and affirming his sentence).

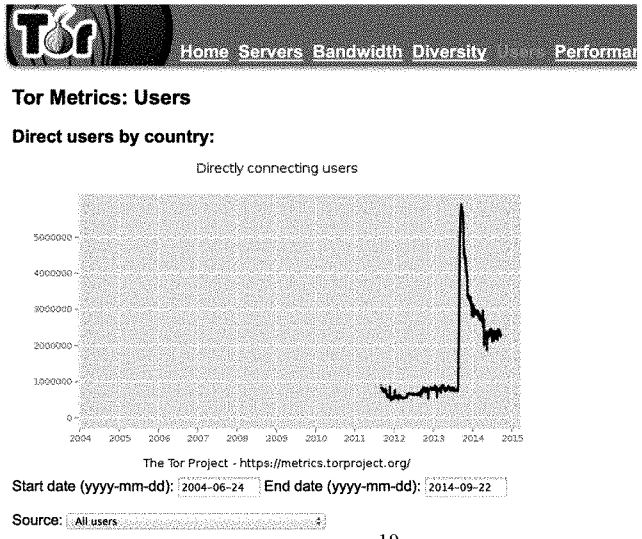

Figure 1. Tor usage over time.[19]

[8] As a result of expanded government surveillance and other trends, such as the rise of Internet use generally and of marketing-oriented and corporate surveillance—the use of online privacy and anonymity protecting tools have risen.[20] For global privacy, a class of online multi-

[19] *TorMetrics—Direct Users by Country*, TOR PROJECT, https://metrics.torproject.org/userstats-relay-country.html?graph=userstats-relay-country&start=2004-06-24&end=2014-09-22&country=all&events=off, *archived at* https://perma.cc/6TPV-73YT (last visited Dec. 3, 2015) [hereinafter *TorMetrics*]; *see also* Karsten Loesing, Steven J. Murdoch, & Roger Dingledine, *A Case Study on Measuring Statistical Data in the Tor Anonymity Network*, FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 203, 210–11 (Radu Sion et al. eds., Springer Berlin Heidelberg 2010), http://sec.cs.ucl.ac.uk/users/smurdoch/papers/wecsr10measuring.pdf, *archived at* http://perma.cc/N5PW-QGP8.

[20] Electronic Privacy Information Center lists 99 such tools, within the following 21 categories: (1) CD/USB Based Operating Systems; (2) Internet Anonymizers, Virtual Private Networks (VPNs), and Proxy Servers; (3) Web Browser Ad-ons; (4) Search Engines; (5) Email Encryption; (6) Alternative Email Accounts; (7) Anonymous Remailers; (8) Disk/File Encryption; (9) Secure Instant Messaging; (10) Disk/File Erasing Programs; (11) Password Vaults; (12) Firewalls; (13) Antivirus; (14) Cookie/Cache/Internet History Cleaners; (15) Mobile Privacy; (16) VoIP/Video Messaging; (17) Social Networking; (18) Meshnet; (19) Alternative Currencies; (20)

jurisdictional anonymity/privacy tools (MJATs))—such as virtual private networks (VPNs), proxy servers, and anonymous networks—have emerged.[21] Examples of these MJATs are JonDo,[22] I2P,[23] Freenet,[24] Lantern,[25] UltraSurf,[26] and TorBrowser.[27] Since 2004, TorBrowser usage has jumped to an average of over 2.5 million daily users worldwide, peaking at over six million users on high-usage days.[28]

[9] MJATs have many uses, and in one way can be thought of as

---

Publishing; and (21) Temporary Mobile Phones. *See EPIC Online Guide to Practical Privacy Tools*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/tools.html, *archived at* https://perma.cc/U4MU-4J5Q (last visited Dec. 3, 2015).

[21] *See id.*

[22] *See JonDo – The IP Changer*, JONDONYM, https://anonymous-proxy-servers.net/en/jondo.html, *archived at* https://perma.cc/4BWJ-YV3S (last visited Dec. 3, 2015) ("You may use JonDonym for anonymous surfing, anonymous e-mail, chats, and other purposes.").

[23] *See What Does I2P Do for You?*, INVISIBLE INTERNET PROJECT, https://geti2p.net/en, *archived at* https://perma.cc/8Z28-2S76 (last visited Dec. 3, 2015) ("I2P is an anonymous overlay network. . .".).

[24] *See Share, Chat, Browse. Anonymously. On the Free Network.*, FREENET PROJECT, https://freenetproject.org/index.html, *archived at* https://perma.cc/GD8T-HDLL (last visited Oct. 4, 2015) ("Share files, chat on forums, browse and publish, anonymously and without fear of blocking or censorship!").

[25] *See Open Internet for Everyone*, LANTERN, https://getlantern.org, *archived at* https://perma.cc/7K8R-FJWK (last visited Oct. 4, 2015) ("Lantern is a free desktop application that delivers fast, reliable, and secure access to the open Internet.").

[26] *See* ULTRASURF, http://ultrasurf.us, *archived at* http://perma.cc/FKX4-7HJZ (last visited Oct. 4, 2015) ("Ultrasurf has now become one of the world's most popular anti-censorship, pro-privacy software. . .").

[27] *See TorBrowser*, *supra* note 1.

[28] *See TorMetrics*, *supra* note 19.

online counter-surveillance tools. In our opening hypothetical, the American journalist and the Australian whistleblower used Tor to evade government surveillance. Many use MJATs simply to evade corporate marketing-driven surveillance.[29] Tor in particular is a source of consternation for the NSA—as revealed by the leaked presentation entitled "Tor stinks."[30] The NSA finds that Tor "stinks" because the NSA cannot break its privacy and anonymity protecting encryption.[31] Like other MJATs, Tor protects individual online privacy and anonymity against government surveillance like the NSA's, or the corrupt Australian LEA's. For this reason, MJATs like Tor are considered high-value targets.[32] The NSA slides portray the typical Tor user as a terrorist, providing them with justification to attack privacy.[33] However, a journalist is just as likely to use anonymity to protect the identity of a whistleblower. Snowden's slides reveal the effort and expense the GIAs invest in breaking Tor.[34] MLATs can uniquely facilitate breaking high-value targets like MJATs—while providing a legal framework for doing so.

[10] Government desire to extend surveillance, coupled with (1) a need to provide a legal framework for otherwise unconstitutional acts (including unlawful intercept and surveillance), (2) the need to pressure CSPs into relaying surveillance information, and (3) the pursuit of MJAT attacks, has led government agencies, LEAs, and others to seek to teach

[29] *See* ULTRASURF, *supra* note 26.

[30] CT SigDev, TOR STINKS, at 1 (June 2012), http://www.slideshare.net/jonbonachon/tor-stinks, *archived at* http://perma.cc/FJ5R-SADX; s*ee also* Ball, Schneier, & Greenwald, *supra* note 9; *42 Years for Snowden Docs Release, Free All Now*, CRYPTOME, https://cryptome.org/2013/11/snowden-tally.htm, *archived at* https://perma.cc/EU9A-HJMK (last updated Aug. 15, 2015).

[31] *See* CT SigDev, *supra* note 30, at 2.

[32] *See id.* at 5.

[33] *See id.* at 15.

[34] *See id.* at 23; s*ee also* Ball, Schneier, & Greenwald, *supra* note 9.

the old MLAT dog new tricks. In this category we demonstrate how MLATs extend government control to foreign CSPs in a way that facilitates a series of technical attacks on online privacy tools.

A. The Expansion of MLATs

[11] We observe the correlation of MLAT expansion with the rise of the Internet, cybercrime, and the expansion of lawful interception, or government surveillance. We note that secret MLAT treaties possibly further expand MLAT proliferation.[35] We observe that the rise in government surveillance—along with the rise in corporate (or civil) surveillance—has driven the proliferation of increasingly more sophisticated online MJATs. Although LEAs form a significant class of MJAT users,[36] GIAs have created an endless cycle of government efforts to attack MJATs and individuals' efforts to defend their privacy. MLATs and MJATs are locked in this endless cycle of cyber arms proliferation.

[12] We then review legal frameworks for intergovernmental legal cooperation, including MLATs: how they work, how many are in force, and which ones are most relevant, as well as frameworks for recognizing and enumerating countries of the world. We demonstrate that recent

[35] *See* Peter Vinthagen Simpson, *Cold War Treaty Confirms Sweden Was Not Neutral,* THE LOCAL (Dec. 9, 2013), http://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-never-neutral, *archived at* http://perma.cc/2RPV-PYMR (regarding revelations following the proliferation of secret treaties); s*ee, e.g.*, Pete Yost, *U.S. Cannot Say How Many Had Communications Watched,* HUFFINGTON POST (July 28, 2011, 5:19 PM), http://www.huffingtonpost.com/huff-wires/20110728/us-surveillance-secrecy/, *archived at* http://perma.cc/N7CR-RYCM (regarding the proliferation of secret legal activity).

[36] *See* arma, *Talking to German Police in Stuttgart*, TOR BLOG (Mar. 26, 2008), https://blog.torproject.org/blog/talking-german-police-in-stuttgart, *archived at* https://perma.cc/FVE2-NAZE; arma, *Trip Report: Tor Trainings for the Dutch and Belgian Police*, TOR BLOG (Feb. 5, 2013), https://blog.torproject.org/blog/trip-report-tor-trainings-dutch-and-belgian-police, *archived at* https://perma.cc/3BDZ-V76X; phobos, *A Visit to Iceland*, TOR BLOG (May 22, 2011) https://blog.torproject.org/blog/visit-iceland, *archived at* https://perma.cc/G2ZT-BDKP.

growth in MLATs has been significantly motivated by a rise in GIA surveillance. We show how the rise of GIA surveillance coincides with the rise of MLATs. We review surveillance and non-surveillance related reasons for the recent increase in MLATs—including a desire to control and compel compliance, anti-bribery enforcement, the ubiquitous war on drugs, and the availability to LEAs of third party corporate surveillance.

B. MLATs and Civil Liberties

[13] First, through Internet-era improvements, which eliminate United States constitutional and other legal protections, the power of MLATs has quietly eroded civil liberties in numerous ways. For example, commentators have pointed out defendants cannot use MLATs,[37] and that MLATs expand unchecked online surveillance.[38] MLATs give rise to numerous civil liberties issues—including eliminating the double jeopardy bar, and the death penalty bar.[39] MLATs have expanded in scope to include political crimes, and eliminate the dual criminality requirements.[40] MLAT enforcement has been presented as compulsory, and the executive branch argues that the courts have no discretion in how the terms of the MLAT are carried out.[41] We note that MLAT surveillance and other

[37] *See* Alastair Brown, *Towards a Prosecutorial Model for Mutual Assistance in Criminal Matters?*, 6 HUME PAPERS ON PUB. POL'Y 50, 52, 56 (1998).

[38] *See Hearing on Law Enforcement Treaties: Hearing Before the S. Comm. on Foreign Relations,* 108th Cong. 39–41(2004) (statement of Marc Rotenberg, President, Electronic Privacy Information Center) [hereinafter *Hearing*].

[39] *See id.* at 40; U.N OFFICE ON DRUGS & CRIME, MANUAL ON MUTUAL LEGAL ASSISTANCE AND EXTRADITION 50–51 (2012), https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf, *archived at* https://perma.cc/QY4G-XS3T.

[40] *See* Inter-American Convention Against Terrorism, art. 11, June 3, 2002, S. TREATY DOC. NO. 107-18; *Hearing*, *supra* note 38, at 40.

[41] Julian Ku & John Yoo, *The Supreme Court Misses Its Chance to Limit the Treaty Power,* FORBES (June 12, 2014, 4:00 AM),

provisions ignore international law. Stepping back, we review the big picture issues MLATs are increasingly raising in the courts: separation of powers, judicial review, and constitutional supremacy.[42]

[14] As MLATs have been enforced—both by the United States in foreign countries and United States MLAT partner countries in the United States—court challenges have proliferated. These cases reflect a growing schism between the executive branch and the courts; with the executive branch asserting that the courts have no role in enforcing constitutional provisions—and some circuit courts have begun to push back. More than thirty years after the Supreme Court decided its last MLAT case—which predated the Internet[43]—an increasing number of MLAT cases have recently reached circuit courts. For example, in *United States v. Getto* the Second Circuit affirmed a conviction after the District Court refused to suppress evidence.[44] The First, Second, Ninth, and Eleventh Circuits have issued contradictory rulings regarding MLATs, and numerous MLAT-related constitutional issues seem ripe for more thorough review by the Supreme Court.[45]

http://www.forbes.com/sites/realspin/2014/06/12/the-supreme-court-misses-its-chance-to-limit-the-treaty-power, *archived at* http://perma.cc/S5Z8-TPB3.

[42] *See Hearing*, *supra* note 38, at 39.

[43] *See* United States v. Alvarez-Machain, 504 U.S. 655, 667–70 (1992).

[44] *See* United States v. Getto (*Getto II*), 586 Fed. App'x. 11, 13 (2d Cir. 2014).

[45] *See, e.g.*, United States v. Moloney (*In re* Price), 685 F.3d 1, 3 (1st Cir. 2012); United States v. Global Fishing (*In* re 840 140th Ave. NE), 634 F.3d 557, 564 (9th Cir. 2010); United States v. Rommy, 506 F.3d 108, 113 (2d Cir. 2007); United States v. Hagege, 437 F.3d 943, 946–47 (9th Cir. 2005); *In re* Comm'r's Subpoenas, 325 F.3d 1287, 1289–90 (11th Cir. 2003); Mercator Corp. v. United States (*In re* Grand Jury Subpoenas), 318 F.3d 379, 381–82 (2d Cir. 2002).

C. MLATs and Legal Frameworks for Global Mass Surveillance

[15] Second, by expanding their legal scope, MLATs have begun to form a legal scaffolding for global surveillance.[46] MLATs can accomplish this either directly or indirectly. On the one hand, they expand scope to explicitly include surveillance.[47] On the other, they create Joint Investigative Task Forces (JITs), which provide potential to circumnavigate restraints on domestic surveillance.[48] JITs can facilitate cooperative surveillance by collaborating with other countries. They can also provide a vector for parallel construction, whereby MLATs are the fig leaves covering up otherwise illegal surveillance.[49] JITs can redefine the investigating party, defining one country's target another country's target. "Cooperative surveillance" has long been performed as a way around domestic spying laws through the use of mutual surveillance by collaborating governments.[50] Additionally, interlocking MLAT cartels of

[46] *See, e.g.*, David Whedbee, Comment, *The Faint Shadow of the Sixth Amendment: Substantial Imbalance in Evidence-Gathering Capacity Abroad Under the U.S.-P.R.C. Mutual Legal Assistance Agreement in Criminal Matters*, 12 PAC. RIM L. & POL'Y J. 561, 561–81 (2003) (arguing that allowing defendants in U.S. criminal proceedings more international access would enhance constitutional protections).

[47] *See Nat'l Cyber Investigative Joint Task Force*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/about-us/investigate/cyber/ncijtf, *archived at* https://perma.cc/6CRP-C4GP (last visited Dec. 3, 2015).

[48] *See id.*

[49] *See* John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013, 3:25 PM), http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805, *archived at* http://perma.cc/ASZ2-KK5Q.

[50] *See id.*

cooperating country LEAs might be tempted to function as super-cartels through legal mechanisms such as JITs.[51]

D. MLATs Expand Technical Automation for Global Mass Surveillance

[16] MLATs facilitate technical expansion of global surveillance in a four-step process. In step one, MLATs help governments establish cooperative control over CSPs.[52] In step two, third parties apply pressure to streamline MLAT requests by automating technical standards and capabilities for government surveillance.[53] In step three, with technical surveillance standards and capabilities, and CSP controls in place, governments can use tools such as XKeyscore to analyze cleartext traffic.[54] In step four, by performing timing and traffic correlation technical attacks against anonymizing tools like MJATs, governments can improve their chances of de-anonymizing encrypted traffic.[55]

[17] In step one, MLATs may play an effective role because

---

[51] *See* Peter Vogel, *The Cloud Privacy Illusion*, E-COM. TIMES (Aug. 8, 2012, 5:00 AM) http://www.ecommercetimes.com/rsstory/75848.html.

[52] *See id.*

[53] *See* ANDREW K. WOODS, GLOBAL NETWORK INITIATIVE, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE 16 (Jan. 2015), https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf, *archived at* https://perma.cc/7A83-FD47.

[54] *See* FRANK SIEPMANN, MANAGING RISK AND SECURITY IN OUTSOURCING IT SERVICES: ONSHORE, OFFSHORE AND THE CLOUD 93–94 (2014), http://www.ittoday.info/Excerpts/Outsourcing_IT_Services.pdf, *archived at* http://perma.cc/M7VK-CWZ2.

[55] *See* Jing Deng, Richard Han, & Shivakant Mishra, *Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks*, *in* FIRST INTERNATIONAL CONFERENCE ON SECURITY AND PRIVACY FOR EMERGING AREAS IN COMMUNICATIONS NETWORKS, at secs. 1, 2 (Inst. of Elec. & Elecs. Eng'rs 2005).

governments exert legal control over CSPs, and therefore network traffic. MLATs formalize this control throughout the world, and set a standard for governments exerting control over CSPs. If a country did not exercise control over its CSPs before entering into a MLAT, as a MLAT signatory, it may now have set an obligation or example, and a standard that, like powerful countries, are expected to do so.

[18] Next, in the context of established, consolidated CSP control, MLATs facilitate implementing a mechanical surveillance roadmap. Third parties use MLATs to facilitate remote surveillance automation.[56] Third parties such as Google are applying pressure via MLATs on telecommunications and data communications service providers to incorporate technical standards which implement automated CSP surveillance. This is turn relieves third parties of legal liability and ongoing complex legal analysis.[57]

[19] Further, through enabling MLAT access to surveillance, third parties hope to stave off increasing pressure from governments around the world to locate local servers within each of their boundaries, subject to local government control.[58] In other words, to preserve their own autonomy, third parties promote the automation of remote surveillance and the strengthening of this legal solution. Presented with the options of either refusing to operate in countries that demand they install local, surveillance-enabled servers, or strengthening those countries' access to surveillance through MLAT-encouraged automation, they choose the latter. However, this results in consequences to citizens living in countries

[56] *See* CTR. FOR INTERNET & SOC'Y, MLATS AND INTERNATIONAL COOPERATION FOR LAW ENFORCEMENT PURPOSES 1–2, http://cis-india.org/internet-governance/blog/presentation-on-mlats.pdf, *archived at* http://perma.cc/7UDL-E2PZ.

[57] *See id.*

[58] *See, e.g.*, Jessica Guynn & David Pierson, *Google Blames Chinese Censors for Outage*, L.A. TIMES (Mar. 31, 2010), http://articles.latimes.com/2010/mar/31/business/la-fi-china-google31-2010mar31, *archived at* http://perma.cc/FF63-MGGT (describing the general conflict between Google and China).

with civil liberties protections, like the United States.

[20] Specifically, corporations urge the use of MLATs to implement technical standards for CSP interfaces—like the European Telecommunications Standards Institute (ETSI) standards[59]—to capture traffic. MLAT-sponsored technical standards form the missing link between legal instruments and actual massive data stores of recorded communications data.[60] Interestingly, not only governments use MLATs for this purpose. Third parties like Facebook collaborate with standards bodies and governments to implement LI technical standards, which are roadmaps for rolling out automated surveillance.[61]

[21] Third parties may collaborate in the technical and legal facilitation of remote Internet-based surveillance for multiple reasons. First, they may seek to reduce and more clearly define the increasing burden of demand for information from LEAs to CSPs. Second, they may want to avoid locating surveillance-enabled servers in foreign countries.[62] Third, they may perceive a need to define the boundaries of legal liability.[63] We analyze a number of documents from third parties, like Google,

[59] *See Who Are Our Members,* EUR. TELECOMM. STANDARDS INST., http://www.etsi.org/about/who-we-are, *archived at* https://perma.cc/manage/create (last visited Sept. 25, 2015) ("We have over 800 members drawn from 64 countries across 5 continents. This reflects the increasing globalization of the communications market and ETSI's key role in enabling it."); *What We Are,* EUR. TELECOMM. STANDARDS INST., http://www.etsi.org/about/what-we-are, *archived at* http://perma.cc/33P2-VKS3 (last visited Sept. 25, 2015) ("We are an independent, not-for-profit organization, widely respected for our neutrality and trustworthiness").

[60] *See Dynamic Triggering*, *supra* note 16.

[61] *See* Shiffman & Cooke, *supra* note 49.

[62] *See* Sarah Cortes, *In Depth: MJAT Jurisdictional Arbitrage Measurement and Technical Experiments* (September 30, 2014) (unpublished manuscript) (on file with author) [hereinafter *In Depth*].

[63] *See id.*

international business consortiums, and international technical standard setting bodies, like ETSI, to MLATs and government surveillance.

E. MLATs Enable New Attacks on Online Privacy and Anonymity Tools

[22] Governments use MLATs to launch attacks and analyze the harvest of information. MLATs work because governments exert legal control over CSPs, as well as network traffic and MJAT traffic.[64] MJATs route traffic all over the world. Once traffic is captured, the third step—analysis of cleartext communications traffic—can begin. For example, NSA XKeyscore surveillance tools appear to fit almost precisely, or "snap in" to work with these standards.[65] Creating paths for network traffic and building circuits that cross jurisdictions can make surveillance by GIAs harder.

[23] Beyond analysis of unencrypted data (with traffic captured) MLATs allow governments of multiple jurisdictions to collaborate in a fourth step to surveillance: performing hitherto challenging or impossible attacks on encrypted or anonymous, privacy-protected communications attacks—such as traffic correlation, traffic analysis, and timing attacks—through multiple countries. We examine this ability of GIAs to perform LI, by using MLATs to defeat constitutional protections to online anonymous communication privacy.[66] In this step, sovereigns use MLATs as a kind of Mutual Lawful Interception Treaties.

[24] MLATs are one of several hostility factors, which governments

[64] *See supra* Part I.d.

[65] *See* Glenn Greenwald & Spencer Ackerman, *How the NSA is Still Harvesting Your Online Data*, THE GUARDIAN (June 27, 2013), http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection, *archived at* http://perma.cc/VQ2D-U8EN.

[66] *See In Depth*, *supra* note 62.

can display to anonymous network communications. Combined with other measurable hostility factors, MLAT risk to MJATs can be quantified per country By becoming jurisdiction-hostility aware, one can improve anonymity by reducing the risk of surveillance through an approach we call "jurisdictional arbitrage."[67] The least hostile countries in which jurisdictional arbitraging privacy tools may concentrate on increasing the proxy servers to expand and disseminate them across the best mix of countries to minimize user risk in the maximum jurisdictions.

[25] Present use of MLATs has become an indicator of legal hostility to freedom in itself. MLATs routinely invalidate the rights of targets. We review measures we have developed to quantify MLAT strength and depth, include "absolute" MLAT hostility and "relative" MLAT hostility. We briefly review other hostility factors.

[26] MLATs provide a metric that, in combination with other metrics, provide a valuable measure of GIA surveillance by country and consequently cause risk to anonymous network communications. In the short term, MJATs can reduce risk by modifying their path selection algorithms to take into account country legal hostility. In the long term, public awareness of the threat to individual privacy can lead to MLAT modifications. Using MLAT attacks to extend law to attack jurisdiction arbitraging privacy tools seems inevitably to result in those tools getting smarter.

[27] We show that traffic may pass through inherently hostile countries with lots of MLATs and large cartels, and apply "absolute" MLAT hostility coefficients to countries. We show the effect when traffic passes through cooperating countries of "relative" MLAT hostility. We review experiments we performed and discuss our methodology. We present the first complete global MLAT map, and discuss new treaties in comparison to accession to existing treaties. We present the results of our experiments and our conclusions: that a high percentage of Tor traffic is at significantly increased risk due to MLATs, and that the risk can be lowered by

[67] *See id.*

rerouting and modifying path selection. We further review Internet Service Providers and Internet Exchange Points (IXPs) and their role as potential surveillance points.

[28] We classify countries according to MLAT and other legal "hostility factors" to Internet freedom in general, and the possibility of deanonymizing MJATs specifically. We develop the first scheme to measure and quantify country-by-country MLAT collaboration, and thus risk, and apply the scheme to create MLAT risk measurements for all countries across the globe. Up to now, researchers have documented a number of technical attacks against MJATs.[68] We now define a new class of attacks, legal attacks, which facilitate the network traffic correlation, traffic timing, and traffic analysis class of attacks. We document a specific new legal attack, the MLAT attack. This allows countries to collaborate and perform a traffic correlation and timing attacks on all cross-jurisdiction MJAT relays or circuits. We show how MJAT traffic risk increases when it passes through countries with high MLAT legal hostility. We present MLATs as one of five surveillance "legal hostility factors" quantified in a related paper.[69] We measure two forms of the MLAT hostility factors: *absolute hostility*, per country MLAT factor; and *collaborative hostility*, MLAT "cartels."[70]

[29] The expansion of MLATs results in MJATs getting smarter.[71] Reducing MLAT score reduces unlawful intercept as a stop to reducing LI. Our recommendations include short-term changes in technology, such as the location of Tor relay nodes. We also recommend long-term changes, such as changing laws involving MLATs and their treaties.

---

[68] *See id.*

[69] *See id.*

[70] *See id.*

[71] *See In Depth*, *supra* note 62.

II. THE QUIET RISE OF MLATS

[30] While MLATs themselves are not new, their numbers and scope have significantly increased since the rise of the Internet—the era when the public has become aware of significantly increased online activity in general, as well as cybercrime and surveillance.[72] "In recent decades, the United States has ratified an increasing number of bilateral treaties with other nations to facilitate legal proceedings, known as mutual legal assistance treaties or MLATs." [73] These proliferating bilateral agreements—such as the EU-US MLAT[74] and the multilateral Budapest Cybercrime Treaty,[75] which were ratified and entered into force in the U.S. in 2010 and 2007, respectively—significantly expand the scope of latitude for LEAs. At the same time, they reduced or eliminated many civil liberties and other privacy protections for individuals.[76]

A. MLAT Mechanics

1. Frameworks for Intergovernmental Legal Cooperation

[31] Since the 20th century, governments have used a number of tools to attempt to obtain cooperation in criminal matters.[77] These tools include:

---

[72] *See id.*

[73] United States v. Global Fishing, Inc. (*In re* 840 140th Ave. NE) 634 F.3d 557, 563 (9th Cir. 2011).

[74] *See* Mutual Legal Assistance Agreement, U.S-E.U, art. 5, June 25, 2003, 43 I.L.M 758 [hereinafter EU-US MLAT].

[75] *See* Council of Europe Convention on Cybercrime, Nov. 23, 2001, 41 I.L.M. 282 [hereinafter *Budapest Cybercrime Treaty*].

[76] *See* Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKLEY TECH. L.J. 425, 438 (2003).

[77] *See* U.N. OFFICE ON DRUGS AND CRIME, MANUAL ON INT'L COOPERATION IN CRIMINAL MATTERS RELATED TO TERRORISM 1 (2009) [hereinafter *See* U.N. MANUAL

- "spontaneous" cooperation[78]
- ad hoc processes through extra-territorial orders from individual countries[79]
- relationships for cooperation outside of MLATs, like the U.S. FBI international "24/7 network"[80]
- national and state statutes[81]
- letters rogatory[82]
- MLAT-type requests such as customs agreements, tax agreements, and others[83]
- bilateral treaties, including extradition, MLAT, and others[84]
- multilateral treaties, including MLAT and others.[85]

[32] Each framework has its strengths and weaknesses. Some are per investigation, some are on a best-efforts basis, some are ad hoc, and some are informal. MLATs reflect an effort to create legally binding agreements to obligate and compel countries to cooperate on criminal investigations and related matters such as target extradition.

ON INT'L COOPERATION].

[78] *See id.* at 63–65.

[79] *See id.*

[80] *See id.*, at 19; s*ee also 24/7 Network of Cyber Investigators Graphic*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/news/stories/2009/january/image/24_7network.jpg/view, *archived at* https://perma.cc/S6WL-SFAZ (last visited Sept. 26, 2015).

[81] *See* U.N. MANUAL ON INT'L COOPERATION, *supra* note 77, at 15–16.

[82] *See id.* at 79, 114–15.

[83] *See id.*

[84] *See id.* at 22.

[85] *See id.*

2. MLAT History

[33] MLATs have existed for quite some time. In the modern era, a U.S. MLAT with Kenya contains documents dating from 1931.[86] The United States signed the first non-secret modern MLAT [87] with Switzerland in 1977.[88] At their most basic, MLATs formally require and enable their signatories to cooperate in many aspects of legal assistance, from investigations, to collection of evidence, to extradition of targets or suspects.

[34] A large and increasing body of case law exists with respect to MLATs. While no case directly holding on issues raised by MLATs has come before the Supreme Court, some such cases bear on MLATs. These include *United States v. Verdugo-Urquidez*, [89] and *United States v. Alvarez-Machain*,[90] a pair of related Mexican cases involving narcotics

[86] *See* U.N. OFFICE ON DRUGS AND CRIME, COMPENDIUM OF BILATERAL, REGIONAL AND INT'L AGREEMENTS ON EXTRADITION AND MUTUAL LEGAL ASSISTANCE IN CRIM. MATTERS KENYA 3 (2010).

[87] This is the first non-secret "modern" U.S. MLAT. Of course, we are not aware of earlier secret MLATs that still remain secret. For an example of a formerly secret treaty which is no longer secret, see Gunnar Rensfeldt, *NSA "asking for" specific exchanges from FRA - Secret treaty since 1954*, SVT.SE (Dec. 8, 2013), http://www.svt.se/ug/nsafra4, *archived at* http://perma.cc/SZ5B-EKJ9.

[88] Treaty between the United States of America and the Swiss Confederation on Mutual Assistance in Criminal Matters, U.S.-Switz., May 25, 1973, 27 U.S.T. 2019, T.I.A.S. 8302 (entered into force Jan. 23, 1977).

[89] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (determining Fourth Amendment protections do not apply to searches and seizures by U.S. agents of property owned by a nonresident alien in a foreign country).

[90] *See* United States v. Alvarez-Machain, 504 U.S. 655, 670 (1992) (holding a defendant's capture by forcible abduction in another country does not prohibit his trial in the U.S. for violations of U.S. laws, and, that the US is not *required* to follow an extradition treaty procedure, that is optional).

involving the murder of a U.S. Drug Enforcement Agency (DEA) official. *Verdugo-Urquidez* established that U.S. Fourth Amendment protections do not apply to searches and seizures by U.S. officials of non-resident, non-citizens in a foreign country, such as those requested in MLATs.[91] *Alvarez-Machain* established that LEAs may operate outside MLATs, and tacitly sanctioned a DEA arrest via illegal abduction.[92]

3. MLAT Classifications

[35] There are multiple kinds of MLATs, and their classification may be viewed along multiple vectors—including signatory scope, category of law, law enforcement goal, treaty focus, criminal threat model, phase, and status. There are multiple sub-options within those classifications. The first vector—signatory scope—may be multilateral (global or regional), bilateral, or unilateral. Multilateral MLATs enshrine agreements between more than two countries.[93] Bilateral MLATs enshrine agreements between two countries.[94] Monolateral MLATs may be considered one-way laws, enacted by some countries to enable them to assist foreign MLA in the absence of actual bilateral agreements with other countries.[95] Regional multilateral MLATs may involve only a handful of countries, while global multilateral MLATs may involve almost every country. A country may enter into both a multilateral MLAT with another country, and a bilateral

[91] *See Verdugo-Urquidez*, 494 U.S. at 275.

[92] *See Alvarez-Machain*, 504 U.S. at 669–70.

[93] *See Definition of Multilateral*, DICTIONARY.COM, http://dictionary.reference.com/browse/multilateral, *archived at* http://perma.cc/T8J8-BMNL (last visited Nov. 30, 2015).

[94] *See Definition of Bilateral*, DICTIONARY.COM, http://dictionary.reference.com/browse/bilateral?s=t, *archived at* http://perma.cc/YAK3-X3ME (last visited Nov. 30, 2015).

[95] *See Definition of Unilateral*, DICTIONARY.COM, http://dictionary.reference.com/browse/unilateral, *archived at* http://perma.cc/BEA6-98AG (last visited Nov. 30, 2015).

treaty with that country, creating legal overlap. Organizations administering multilateral MLATs include the E.U., the Council of Europe, the U.N., the Organization for Economic Cooperation and Development, the Association of Southeast Asian Nations, and the Organization of American States.[96]

[36] Naturally, not all MLATs are created equal. Some multilaterals MLATs are not directly enforceable in the member states.[97] Instead, signatories are required to adopt laws or procedures which have the desired effect and are enforceable. For example, in the United Nations Convention Against Illicit Trafficking Narcotic Drugs and Psychotropic Substances, "signatories are required to [implement laws or] procedures which will enable the signatories' own authorities to 'identify, seize, and freeze' proceeds or property derived from illegal drug activities."[98] For this reason, bilateral treaties are considered significantly stronger than many multilateral treaties.

[37] A treaty's category of law may be either civil or criminal, as some MLATs deal with civil law and others with criminal law. We concern ourselves primarily with criminal MLATs or MLAT provisions. The law enforcement goal of treaties may include extradition (or what some call a rendition) or non-extradition mutual legal assistance. Extradition or rendition treaties are often viewed as separate from MLATs, but they are

[96] *See, e.g.*, Dep't of Int'l Law, *Inter-American Convention on Mutual Assistance in Criminal Matters Preamble*, ORG. OF AM. STATES, http://www.oas.org/juridico/english/treaties/a-55.html, *archived at* http://perma.cc/HC2Z-MGCE (last visited Dec. 3, 2015).

[97] *See* Thomas F. McInerney III, Note, *Towards the Next Phase in International Banking Regulation*, 7 DEPAUL BUS. L.J. 143, 164–65 (1994) (stating "[a]lthough not self-evidently applicable, the Drug Convention may supply some needed assistance in developing a truly multilateral solution to the problem of illicit bank activities. . . Although not directly enforceable in the member states.").

[98] *Id.* (quoting United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances art. 5, Dec. 20, 1988, 28 I.L.M.493).

closely related.[99]

[38] In the fourth category, treaty focus, a treaty may be either simply a general MLAT, or it may have MLA provisions incidental to other treaty foci. Examples include tax agreements, customs agreements, Hague Convention on Child Abduction,[100] and Schengen Acquis Treaty.[101]

[39] Motivation for a number of MLATs has been linked to campaigns against specific crimes.[102] These MLATs may be narrow, and may overlap with other MLATs. Criminal threats—the fifth MLAT classification vector—may include one or more specific criminal threats. These may include narcotics, anti-bribery, human trafficking, skyjacking, organized crime, terrorism, weapons trafficking (including nuclear weapons), or tax evasion incident to banking secrecy laws.

[40] MLATs typically take five to ten years to develop between a few principal phases.[103] For this reason, attempts to identify treaties by date

---

[99] *See Definition of Extradition Treaty*, THE FREE DICTIONARY, http://legal-dictionary.thefreedictionary.com/Extradition+treaty, *archived at* http://perma.cc/257D-QRMQ (last visited Nov. 30, 2015).

[100] *See* Hague Convention on the Civil Aspects of International Child Abduction, Oct. 25, 1980, T.I.A.S. No. 11670.

[101] Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (Schengen Acquis Treaty), June 14, 1985, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:42000A0922(01), *archived at* http://perma.cc/6M29-VJNY.

[102] *See, e.g.*, Brian Kindle, *MLATS Are Powerful Weapons in Financial Crime Combat, Even for Private Sector*, ASSOC. OF CERTIFIED FINC. CRIM. SPECIALISTS, http://www.acfcs.org/mlats-are-powerful-weapons-in-counter-financial-crime-combat-even-for-private-sector/, *archived at* http://perma.cc/8284-Y86Z (discussing MLATs specific to financial crimes).

[103] *See generally* Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC. L.J. (Jan. 28, 2015 1:05 PM), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/, *archived at* http://perma.cc/VE9Y-2CVV.

can result in greater confusion. We classify MLATs by a sixth vector—phase—to clarify whether and where it may be in force. Phases include drafting, signing, acceptance, approval, ratification, deposit of instrument, accession, and entry into force. These can all happen on different dates, or the same date, depending on the treaty.

[41] Only in the last of these phases is the MLAT actually in effect, a status often referred to as "treaty in force."[104] For this and other reasons, such as expiration or a country ceasing to exist, a treaty may have a status of "not in force."[105] Another issue with MLATs is finding definitive sources and agreeing on a definitive citation. As they are by nature signed by at least two parties, each party may claim to hold the definitive reference. Not to mention each treaty has multiple versions on its long journey from drafting to entry into force.

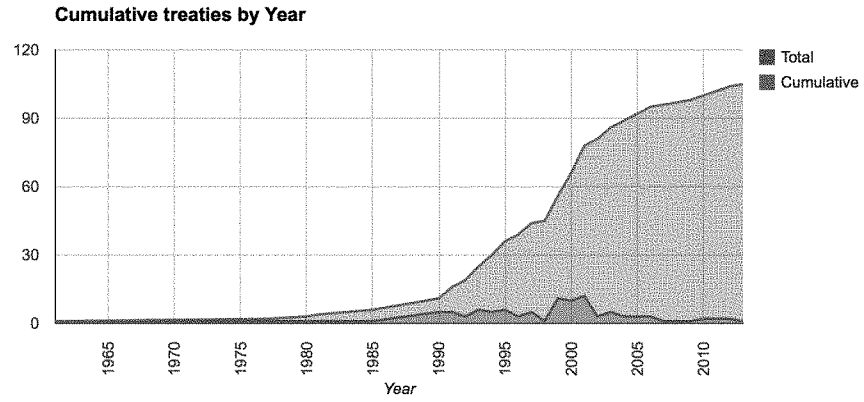

Figure 4. India, U.S., and U.S. MLAT growth.[106]

[104] *See Definition of Treaties in Force*, THE FREE DICTIONARY, http://legal-dictionary.thefreedictionary.com/Treaties+in+Force, *archived at* http://perma.cc/69AG-3F6S (last visited Nov. 30, 2015).

[105] *See What is Entry Into Force?*, THE EUCLID TREATY, http://www.euclidtreaty.org/what-is-entry-into-force/, *archived at* http://perma.cc/Y7RN-V368 (last visited Dec. 3, 2015).

[106] *See* Sarah Cortes, *MLAT Database* (unpublished research results) (on file with author).

4. MLAT Measurement – The MLAT Database

[42] In this article, we perform the first comprehensive and global analysis of MLATs. From original sources, we have constructed what is—to our knowledge—the first complete database of all MLATs, providing the first MLAT big picture. Between 1977 and 2013, the number of MLAT relationships between all countries grew from a few to several hundred.[107] During this period, the number of participating countries grew also.[108] Between the U.S., and the U.K. alone treaties grew from 1 to 105.[109]

[43] MLAT analysis shows that new adversarial models are necessary to take into account global surveillance, and that different governments may pose different, quantifiable risks to civil liberties and anonymous network communications, based on observable factors such as MLATs in force. The database consists of 32 tables and reports. Tables capture links to the original documents, the official source repository for the document, lists of signatory countries, dates, and any other available information. Some tables capture multilateral treaty information, and others capture bilateral treaty information. We summarize the various treaties and treaty sets in a summary table.

[44] We use the ISO 3166 standard to identify 191 autonomous governments in the world.[110] A set of scripts loop through various tables to

[107] *See id.*

[108] *See id.*

[109] *See id.*

[110] *See Country Codes – ISP 3166*, INT'L ORG. FOR STANDARDIZATION, http://www.iso.org/iso/country_codes, *archived at* http://perma.cc/8HX6-WWQT (last visited Dec. 3, 2015) (stating "ISO 3166 is the International Standard for country codes and codes for their subdivisions."). As of October 4, 2015, ISO 3166 recognized 249 "countries." *Online Browsing Platform*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/obp/ui/#search (last visited Oct. 4, 2015); s*ee also ISO 3166-1*,

create summaries and reports, including total number of treaties entered into by countries, and which countries have treaty relationships with each other. We then bring to light *MLAT cartels*, groups of countries that have entered into treaty relationships with each other, whose LEAs may cooperate. We provide for treaty risk weights to experiment with different scoring algorithms.

B. Motives for MLAT Growth and Expansion

1. Roots Combatting Money Laundering

[45] Mark M. Richard—the Deputy Assistant Attorney General of the Criminal Division—testified to the advantages of MLATs over letters rogatory to the House Foreign Affairs Committee in 1987.[111] He stated "an MLAT, either by itself or in conjunction with domestic implementing legislation, can provide a means of overcoming bank and business secrecy laws that have in the past so often frustrated the effective investigation of large-scale narcotics trafficking operations."[112]

[46] In the 1970s, against a backdrop of bank secrecy laws and the emergence of offshore tax havens, the rise of the Internet saw a rise in money laundering crimes, including the two largest categories, narcotics-

---

WIKIPEDIA.ORG, https://en.wikipedia.org/wiki/ISO_3166-1#cite_note-6, *archived at* https://perma.cc/EP4D-XDTN (last modified Aug. 10, 2015). The U.N. recognizes and maintains a list of sixty-nine Trust and Non-Self-Governing Territories; however, twenty-one of these have no separate country code and are not listed in ISO 3166. *See Country Codes – ISP 3166*, INT'L ORG. FOR STANDARDIZATION, http://www.iso.org/iso/home/standards/country_ codes.htm (last visited Sept. 23, 2015). So, the total number of countries with autonomous or semi-autonomous governments in the world today can be evaluated as 201 countries.

[111] *See Worldwide Review of Status of U.S. Extradition Treaties and Mutual Legal Assistance Treaties: Hearing Before the H. Comm. on Foreign Affairs*, 100th Cong. 26 (1987) (statement of Mark M. Richard, Deputy Assistant Attorney General, Criminal Division).

[112] *Id.* at 37.

and bribery related crimes.[113] This partially drove MLAT expansion after 1977. Complex international cases—notably, one concerning commodities trader Marc Rich, then the largest tax evasion case in U.S. history—drove the U.S. Department of Justice to seek more formal methods to gain international cooperation and legal assistance from other governments.[114]

[47] Since then, an increasing number of MLATs have been implemented around the world. Treaty growth is driven by a number of factors, including both government and corporate agendas. The latter include the desire to expand business abroad unfettered by bribery demands and—more recently—legal uncertainties regarding CSP obligations to provide subscriber information to LEAs. Corporate anti-bribery initiatives played a significant motivating role in the expansion of MLATs in recent decades. The poorest countries may be the most frequent targets of enforcement.[115]

[48] Choi and Davis found that "at the country level we report evidence that the SEC and DOJ impose greater aggregate sanctions for violations in countries with a lower per capita and weaker local anti-bribery institutions."[116] Further, this skew may not be related to a higher

---

[113] *See History of Anti-Money Laundering Laws*, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/news_room/aml_history.html (last visited Sept. 22, 2015). S*ee also The Critical Connection Between the Internet and Money Laundering,* RED EARTH INTEL, Jan. 1, 2015, http://www.redearthintel.com/1/post/2015/ 01/the-critical-connection-between-the-internet-and-money-laundering.html; *Country Codes – ISP 3166*, *supra* note 110.

[114] *See* ETHAN A. NADELMANN, COPS ACROSS BORDERS: THE INTERNATIONALIZATION OF U.S. CRIMINAL LAW ENFORCEMENT 338 (1993).

[115] *See* Stephen J. Choi & Kevin E. Davis, *Foreign Affairs and Enforcement of the Foreign Corrupt Practices Act* 14 (N.Y.U. Sch. of Law Pub. Law & Legal Theory Research Paper Series, Working Paper No. 12-35, Law & Economics Research Paper Series, Working Paper No. 12-15, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2116487, *archived at* http://perma.cc/DV4J-AFGQ.

[116] *Id.* at i.

prevalence of guilt by poorer countries, as Choi and Davis go on to conclude: "overall, these findings suggest that factors besides those deemed relevant by U.S. and international law influence enforcement of the FCPA."[117] For example, the OECD treaties—where Asian countries predominate—reflect an emphasis on reducing the cost of doing business (i.e., the cost of bribes) for wealthy companies leveraging profits in poor countries.[118]

[49] Sadly, MLATs and other tools failed to recover the estimated $5 billion the Marcoses laundered out of the Philippines—mainly to Swiss banks[119]—or to provide restitution or justice to their victims of domestic terror.[120]

2. Returning the Favor: Performance Certainty

[50] Fed up with years of lacking assistance from other governments in the pursuit of bank secrecy targets like Marc Rich, the U.S. DOJ first negotiated MLATs—like the 1977 one with Switzerland—to have teeth in compelling other governments to cooperate and assist.[121] Thirty years later, their success demonstrated apparent but unintended consequences for Boston College academics. ACLU of Massachusetts summed up in its brief:

> [t]he government . . . maintains that the Applicants are not

---

[117] *Id.*

[118] *See* ADB/OECD ANTI-CORRUPTION INITIATIVE FOR ASIA AND THE PACIFIC: MUTUAL LEGAL ASSISTANCE, EXTRADITION AND RECOVERY OF PROCEEDS OF CORRUPTION IN ASIA AND THE PACIFIC 25 (2007).

[119] *See* David Chaikin, *Tracking the Proceeds of Organised Crime – The Marcos Case*, AUSTL. INST. OF CRIMINOLOGY, Mar. 9–10, 2000 at 4–5.

[120] *See* Philippines v. Pimentel, 553 U.S. 851, 854 (2008).

[121] *See* Mutual Assistance in Criminal Matters, U.S.-Switz., May 25, 1973, 27 U.S.T. 2019, T.I.A.S. No. 8302 (entered into force 1977).

> entitled to any judicial review. In the government's view, the Mutual Legal Assistance Treaty between the U.S. and the U.K. authorizes a foreign power, acting with the Executive's unreviewable stamp of approval, to compel citizens to produce confidential information for prosecutions abroad.[122]

[51] Countries also sought to ensure performance certainty with MLATs. For instance, the Eleventh Circuit reversed an order overruling MLAT compliance with a request from Canada regarding a smuggling operation, holding that "MLATs . . . have the desired quality of compulsion as they contractually obligate the two countries to provide to each other evidence and other forms of assistance needed in criminal cases," [123] both during pre-charge investigation and post-charge prosecution stages.[124] The court also ruled that

> despite the apparent versatility of 28 U.S.C. § 1782—titled "[a]ssistance to foreign and international tribunals and to litigants before such tribunals—law enforcement authorities found the statute to be an unattractive option in practice because it provided wide discretion in the district court to refuse the request and did not obligate other nations to return the favor that it grants."[125]

[52] Press coverage of the First Circuit missed the point that MLAT treaty compliance is intended by its drafters to be non-discretionary.[126]

---

[122] Br. for Ed Moloney & Anthony McIntyre as Amici Curiae Supp. Appellants at 6, United States v. Maloney (*In re* Price), 685 F.3d 1 (1st Cir. 2012) (No. 11-2511) [hereinafter Br. for Ed Maloney].

[123] *In re* Comm'r's Subpoenas, 325 F.3d 1287, 1290 (11th Cir. 2003).

[124] *See id.*

[125] *Id.*

[126] *See* United Kingdom v. Trs. of Bos. Coll., 718 F.3d 13, 23 (1st Cir. 2013).

Those that grasped this argued that the Boston College Trustees should have challenged this point more strenuously, and pursued the request to the court to quash the subpoenas on grounds of academic freedom, among others.[127] We discuss this case in further detail later.[128]

[53] Regarding MLAT performance certainty, Senator John Kerry—ironically a member since 1990 of the same Senate Foreign Relations Committee that approved MLATs, including Chair from 2009–2013, and now Secretary of State himself—wrote a letter regarding *Trustees of Boston College* to the then Secretary of State Hillary Clinton.[129] In that letter, he wrote:

> Given my deep concern, I spoke to Attorney General Holder about this matter late last year. I fully recognize that the United Kingdom has invoked the provisions of our Mutual Legal Assistance Treaty and that this is clearly a factor that affects our flexibility dealing with such a request. Nonetheless, given the close relationship we have with the United Kingdom and the deep and enduring interest all of us share in seeing a lasting peace in Northern Ireland, I would urge you to work with the British authorities to reconsider the path they have chosen and revoke their request.[130]

---

[127] *See, e.g.*, Ed Moloney, *Ed Moloney: Boston College and Me*, BOS. COLL. SUBPOENA NEWS (Aug. 11, 2014), https://bostoncollegesubpoena.wordpress.com/2014/08/11/ed-moloney-boston-college-and-me/; *Country Codes – ISP 3166*, *supra* note 110.

[128] *See* discussion *infra* Part II.B.3.

[129] Letter from John Kerry, Sen., U.S. Cong., to Hilary Clinton, Sec'y of State, U.S. State Dept. (Jan. 23, 2012).

[130] *Id.*; *see also* Ross Kerber, *Kerry Reaches out on Northern Ireland "Troubles" Records*, REUTERS (Jan. 27, 2012, 5:47 PM), http://www.reuters.com/article/2012/01/27/us-usa-britain-ira-idUSTRE80Q27R20120127?feedType=RSS&feedName=everything&virtualBrandChannel=11563, *archived at* http://perma.cc/9QYJ-WKDC.

No one knew better than Kerry, since he—ironically, as Chair—approved the US-UK-MLAT that voluntarily tied its own hands.[131] It was to Kerry's committee that Rotenberg had addressed his apparently unheeded 2004 testimony.[132]

[54] MLATs strictly compel parties targeted for investigation to perform under the MLAT, but do not seem to likewise compel the Attorney General to require enforcing countries to conform to MLAT terms. In *Boston College Trustees*, the government attempts to argue just that, stating:

> [T]his Court affirmed in *In re: Request*, the US-UK MLAT by express terms precludes a private party from refusing to comply with a request for production of documents on the ground that the requirements of the treaty have not been followed. Thus, even if Price's death did call into question whether the United States was still required to provide the documents to the UK pursuant to the treaty, which it does not, that would not absolve Boston College of its obligation to provide the documents to the United States and this appeal would remain viable.[133]

[55] The First Circuit has cited the US-UK MLAT in ruling it allows the US Attorney General to decide to pursue a request despite noncompliance with treaty terms: "Treaty is intended solely for mutual legal assistance between the parties. The provisions of this Treaty shall not give rise to a right on the part of any private person to obtain, suppress, or

---

[131] *See* Mutual Legal Assistance Treaty, U.S.-U.K., art. I, Jan. 6, 1994, T.I.A.S. 96-1202 (1995) [hereinafter US-UK MLAT].

[132] *See Hearing*, *supra* note 38.

[133] Gov't's Opp. to Bos. Coll.'s Mot. to Dismiss its Appeal as Moot, at 9, United States v. Trs. of Bos. Coll., 718 F.3d 13 (1st Cir. 2013) (No. 12-1236) (citing United States v. Moloney (*In re* Price), 685 F.3d 1, 12–13 (1st Cir. 2012)).

exclude any evidence, or to impede execution of a request."[134]

3. Executive v. Judicial Branches

[56] There can be little doubt, when reviewing current court cases and government briefs, that our executive branch views MLATs as a general strategy to expand its powers and enable law enforcement aims to supersede constitutional protections when reviewing current court cases and government briefs. Having attempted to remove judicial discretion from the treaties, the government's position since then has been to convince the judicial branch of its resulting lack of power to enforce constitutional protections. For example, in *Boston College Trustees*, the Court summarizes the Executive Branch's position:

> The government, for its part, contends that courts do not have discretion under the US–UK MLAT to review for relevance materials subject to a subpoena. It states that only the Attorney General, not the courts, has discretion to decline, delay or narrow a request under the treaty. . . . Pursuant to Article 3 of the US–UK MLAT, it is the Attorney General who decides whether to accede to a request from the UK, to narrow compliance to a certain aspect of said request or to decline to cooperate altogether. The government, however, erroneously concludes that the Attorney General's exclusive prerogative in initiating proceedings translates into a general bar on judicial oversight of the subpoena enforcement process.[135]

[57] The court in *Commissioner's Subpoenas* also noted "United States courts have consistently ruled that similar provisions in other treaties do not important substantive constitutional or statutory protections into the

[134] *In re* Price, 685 F.3d at 11–12; s*ee also* US-UK MLAT, *supra note* 131, at art. I.
[135] United Kingdom v. Trs. of Bos. Coll., 718 F.3d 13, 20–21 (1st Cir. 2013) (internal citations omitted).

extradition context."[136] It concluded

> [p]rior cases involving similar language in other treaties further illustrate that vague and general references to the 'law of the Requested State' in treaties must be carefully construed in the context of all the language of the Treaty and cannot simply be read in mechanical fashion as the appellees contend . . . .[137]

The court goes on to cite *Elcock v. United States*—an extradition treaty case—which, while distinguishable, found:

> Had the parties intended that each would apply its own [substantive] law in determining whether the requested extradition would violate double jeopardy principles, they could have clearly stated as much....In the absence of such a provision, a court may not simply rely on the meanings the terms of the treaty have in the context of domestic law.[138]

Additionally, the Second Circuit established that the U.S. government may conduct investigations and obtain evidence outside MLAT provisions.[139]

---

[136] *In re* Comm'r's Subpoenas, 325 F.3d at 1303 (citing Elcock v. United States, 80 F. Supp. 2d 70, 77 (E.D.N.Y. 2000)).

[137] *In re* Comm'r's Subpoenas, 325 F.3d at 1302.

[138] *Elcock*, 80 F. Supp. 2d at 77. Elcock robbed a bank in Germany with his girlfriend accomplice, concealed over $419,000 in a teddy bear, and mailed it to his sister in the U.S. He was arrested and convicted in New York shortly thereafter, when he arrived to visit his sister, and accepted delivery of the teddy bear. *Elcock* is also interesting constitutionally, as it permitted extradition in an apparent double jeopardy case (related not to an MLAT, but an extradition treaty), as Germany sought to prosecute him after his U.S. conviction.

[139] United States v. Rommy, 506 F.3d 108, 128–29 (2d Cir. 2007). Dutch national Henk Rommy, also known as the "Cobra," headed an international drug ring that trafficked in large quantities of controlled substances like "ecstasy"... [Co-conspirators] testified that the pills in question were light blue in color and stamped with the logo of the late Italian

[58] The little noticed 2003 Eleventh Circuit case *In re Commissioner's Subpoenas* [140] already provided the grounds on which Rotenberg's prophecy for the Budapest Cybercrime Treaty would come true:[141] that "vague and general references" to legal protections offer scant protection to privacy and other civil liberties in treaties.[142]

[59] Perhaps noting the ease with which the judicial branch sustained the executive branch's inclination to deprioritize civil protections, we see that an increasing number of treaties explicitly exclude civil liberties in recent years.[143]

[60] However, cases are currently working their way through the courts in which they take responsibility for review of MLAT requests, reasserting judicial review and the supremacy of the Constitution.[144] The executive branch continues to fight back on these efforts, through government appeals

4. Surveillance-Related Motives: Governments

fashion designer Gianni Versace...[Romy] had smuggled the drugs in recreational vehicles shipped from Europe . . . into New York. *Id* at 111; s*ee also* Treaty on Mutual Assistance in Criminal Matters, U.S.-Neth., art. 18, § 1, June 12, 1981, 35 U.S.T. 1361 (1981).

[140] *See generally In re* Comm'r's Subpoenas, 325 F.3d 1287 (11th Cir. 2003) (holding that a request under a mutual legal assistance treaty is not reviewable by a district court).

[141] *See* Br. for Ed Moloney *supra* note 122, at 22. *See generally Budapest Cybercrime Treaty*, *supra* note 75.

[142] *See Hearing*, *supra* note 38, at 39–41; *In re* Comm'r's Subpoenas, 325 F.3d at 1302.

[143] *See Trs. of Bos. Coll.*, 718 F.3d at 20–21.

[144] *See, e.g.*, United States v. Maloney (*In re* Price), 685 F.3d 1 (1st Cir. 2012).

[61] An examination of treaties—including the EU MLAC,[145] the EU-U.S. MLAT,[146] and the multilateral Budapest Cybercrime Treaty[147]—reveals their emphasis on surveillance, including online and telecommunications. While MLATs have been used to proliferate surveillance mechanically—they have also served to provide a little-observed legal basis for global surveillance by GIAs.

[62] Was extending surveillance globally a key motivating factor behind recent MLATs, or a by-product? For the answer to that question, we need look no further than public testimony by its drafters, on which the 2011 *Global Fishing* decision places so much emphasis.[148] For example, in 2005, Mary Ellen Warlow—the Director of the Office of International Affairs, Criminal Division, U.S. Department of Justice—made a statement before the Senate Committee on Foreign Relations concerning law enforcement treaties.[149] She testified:

> [T]his is the first United States MLAT to include special investigative techniques among permissible types of

---

[145] *Convention on Mutual Assistance in Criminal Matters Between the Member States of the European Union* (Dec. 2011), 2000 O.J. (C 197) 1 (EU) [hereinafter EU MLAC], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:C2000/197/01&from=EN, *archived at* http://perma.cc/87TK-5JE4.

[146] EU-ES MLAT, *supra* note 74.

[147] Council of Europe (C.O.E.): Convention on Cybercrime, Nov. 23, 2001, 41 I.L.M. 282.

[148] United States v. Global Fishing, Inc. (*In re* 840 140th Ave. NE), 634 F.3d 557, 563 (9th Cir. 2011).

[149] *Statement of Mary Ellen Warlow, Director, Office of International Affairs, Criminal Division, U.S. Department of Justice: Hearing Concerning Law Enforcement Treaties Before the S. Comm. on Foreign Relations,* 109th Cong. (2005), http://www.state.gov/documents/organization/87297.pdf, *archived at* http://perma.cc/72C7-2NC5.

> assistance. Specifically, Article 12 establishes that the Parties may use telecommunications surveillance, undercover investigations, and controlled deliveries, in accordance with their domestic law, in execution of requests for assistance. This provision was included at Germany's request, to assert the Federal government's legal authority, through the States, to undertake such actions on behalf of foreign authorities.[150]

Samuel M. Witten—the Deputy Legal Adviser for the U.S. Department Of State—further testified before the Committee on "An Extradition Treaty With Great Britain And Northern Ireland, . . . Israel, . . . Germany, and . . . Japan,"[151] stating:

> The proposed U.S.-Germany Mutual Legal Assistance Treaty in Criminal Matters (MLAT) fills a significant gap in our network of MLATs with major European law enforcement partners . . . . The MLAT with Germany is typical of our over 50 MLATs with countries around the world, including most of the countries of Europe. It has several innovations, including provisions on special investigative techniques, such as telecommunications surveillance, undercover investigations, and controlled deliveries. It allows certain uses for evidence or information going beyond the particular criminal

[150] *Id.* at 10.

[151] *Testimony by Deputy Legal Adviser, Department of State, to Senate Foreign Relations Committee regarding certain bilateral law enforcement treaties, U.S. Senate: Hearing on an Extradition Treaty with Great Britain and Northern Ireland, an Extradition Protocol with Israel, Mutual Legal Assistance Treaty with Germany, and a Mutual Legal Assistance Treaty with Japan Before the S. Committee on Foreign Relations,* 109th Cong. (2005) (statement of Samuel M. Witten, Deputy Legal Adviser, U.S. Dep't of State), http://www.state.gov/s/l/2005/87190.htm, *archived at* http://perma.cc/5STL-UXDW.

> investigation or proceeding. . . .[152]

[63] Broad surveillance provisions are found in every MLAT of this era. For example, Title III of the EU MLAC explicitly and in detail authorizes the use of "Interception of Telecom."[153] Article 20 is noted for its implications: "[i]nterception of telecommunications without the technical assistance of another Member State."[154] Surveillance has been automated to the point where Member State assistance in surveillance is no longer operationally necessary.[155]

[64] By contrast, the Inter-American Convention on Mutual Assistance in Criminal Matters—which has more than 20 signatory states—specifically mentions neither telecommunications interception nor surveillance.[156] The Budapest Cybercrime Treaty contains extensive provisions for surveillance of real time metadata, as well as content.[157] This extends to a requirement that signatories conceal the fact of surveillance: "[e]ach Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information related to it."[158]

---

[152] *Id.*

[153] *See* EU MLAC, *supra* note 145.

[154] *Id.* at 13.

[155] *See Dynamic Triggering*, *supra* note 16.

[156] *See* Organization of American States, Inter-American Convention on Mutual Assistance in Criminal Matters, May 23, 1992, O.A.S. No. 75, http://www.oas.org/juridico/english/treaties/a-55.html, *archived at* http://perma.cc/2TU8-EZ9V.

[157] *See Budapest Cybercrime Treaty*, *supra* note 75 at tit. 5, art. 20–21.

[158] *Id.* at art. 20, section 3.

[65] The EU-U.S. MLAT—into which parties entered negotiations shortly after 9/11, and which entered into force in 2010—provides broad powers that include surveillance.[159] It provides, "[m]utual [...] assistance shall be afforded to a national administrative authority," investigating matters for a criminal prosecution could include requests for surveillance or the interception of communications.[160] Under Article 7, broad requests can be made by "fax or e-mail, with formal confirmation to follow when required by the requested State."[161]

[66] Referring to Article 5, Section 3, StateWatch.org commented:

> EU law enforcement officers in the joint teams from the state where the operation is being conducted will be allowed to circumvent formal requests for mutual assistance by directly requesting surveillance by other national agencies, the interception of telecommunications, search warrants, arrest and detention. No mechanisms for accountability are set out.[162]

5. Surveillance-Related Motives: Third Parties

[67] Third parties play an important role in pushing the expansion of MLATs.[163] Dramatic increases in requests to third parties for otherwise private communications has led to their collaboration in implementing technical standards and capabilities for surveillance. We summarize

[159] *See* EU-US MLAT, *supra* note 75.

[160] *Id.* at 16.

[161] *Id.* at 15.

[162] *EU: JHA Council authorises signing of EU-USA agreements on extradition and mutual legal assistance*, STATEWATCH.ORG (June 5, 2003), http://www.statewatch.org/news/2003/jun/01useu.htm, *archived at* http://perma.cc/YG4A-WTGP.

[163] *See Dynamic Triggering*, *supra* note 16.

briefly here.

[68] Responding to pressure from governments around the world for access to subscribers' private data and communications, third parties like Facebook have lobbied to implement technical standards facilitating surveillance through MLATs.[164] In this way, MLATs play a quiet role in mandating technological solutions to facilitate government surveillance.

[69] Through ETSI standards, like ETSI Technical Standard 102 677,[165] third parties have sought to incorporate CSP Lawful Intercept technical design and infrastructure standards and requirements into MLATs, to facilitate remote surveillance automation.[166] It appears from various treaty provisions that this automation has been taken into account, and is assumed. For example, Article 20 of the EU MLAC covers Interception of Telecommunications *without* the technical assistance of Another Member State.[167]

[70] MLATs also invoke action immediately upon ratification in another sense: the requirement to implement specific legislation—including international technical standards like ETSI TS 102 677—which details dynamic triggering" for fully automated "lawful" interception (i.e., surveillance).[168] Another interesting standard is *ETSI TS 187 005,*

[164] *See id.*

[165] *See generally ETSI DTS 102 677 V0.4.1 (2010-03), Lawful Interception (LI); Dynamic Triggering; Dynamic Triggering of Content of Communication Interception, Work Item: DTS/LI-00058,* ELEC. TELECOMMS STANDARDS INST. (Mar. 2010) (defining the standard), http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_LI/2010_37_NYC/SA3LI10_049.doc (automatic download) (detailing the technical design and infrastructure standards for communication service providers (CSP) and dynamic triggering across multiple operators) [hereinafter *ETSI DTS 102 677*].

[166] *See Dynamic Triggering*, *supra* note 16.

[167] Convention on Mutual Assistance in Criminal Matters Between the Member States and the European Union, *supra* note 156, at 13–14.

[168] *See* ETSI DTS 102 677, *supra* note 165.

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Stage 1 and Stage 2 definition.[169]

[71] Others have documented extensive collaboration by telecommunications and other third parties on purveying information to the U.S. government.[170] However, the collaboration by third parties with foreign GIAs through MLATs has received scant attention. How collaboration with non-U.S.-countries can impact U.S. citizens has also received scant attention.

[72] In the past, evidence was collected by law enforcement agencies. When one government LEA sought evidence from another jurisdiction, it generally sought it from the other jurisdiction's LEA. But with the advent of electronic communications, foreign governments are increasingly seeking evidence from foreign third parties—mostly U.S. third parties like Google, Twitter, and Facebook. The increasing demands on third parties for access to subscribers' personal communications information has effectively compelled third parties like Facebook to exert pressure to expand MLATs, in order to set boundaries for this demand.[171] Hosein and Banisar observed of the then-draft Budapest Cybercrime Treaty that "[its]

---

[169] *See generally* ETSI *DTS 187 005 V3.1.1 (2012-06), Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Stage 1 and Stage 2 definition,* ELECTRONIC TELECOMMS STANDARDS INST. (June, 2012) [hereinafter *ETSI DTS 187 005*], http://www.etsi.org/deliver/etsi_ts/187000_187099/187005/03.01.01_60/ts_187005v030101p.pdf, *archived at* http://perma.cc/2D9Q-NTHH (defining and specifying, when the network supplying services on behalf of the communication service provider is a next generation network, stage 1 and stage 2 of interception capability and the stage 2 model for lawful interception).

[170] *See NSA Spying on Americans*, ELEC. FRONTIER FOUND., https://www.eff.org/nsa-spying, *archived at* https://perma.cc/6SQ5-RXR3 (last visited Oct. 1, 2015).

[171] *See Global Government Surveillance Reform,* REFORM GOV'T SURVEILLANCE, https://www.reformgovernmentsurveillance.com/index.html, *archived at* https://perma.cc/H4MS-8ABA (last visited Oct. 1, 2015).

requirements are extremely expansive in scope, and impose significant burdens on Internet providers, operators, users and equipment manufacturers to collect information, conduct surveillance and provide assistance."[172]

[73] The recent increase in corporate transparency reports and takedown demands documents this. In the first six months of 2013, petitioners from almost 100 countries had submitted almost 25,000 takedown requests to Google alone.[173] Transparency reports from Microsoft,[174] Twitter,[175] Facebook,[176] and others report similar trends. The desire by these third parties to set boundaries on these requests is a key driving factor behind the involvement of CSP in MLATs. In becoming so involved, third parties found themselves drawn deeper and deeper into MLAT surveillance collaboration. This resulted in a marriage between not only the global CSPs and U.S. surveillance interests like the NSA, but GIAs of all countries.

[74] A number of documents reveal the extent of this corporate involvement. By September 2012, the International Chamber of Commerce (ICC)[177] was drafting detailed recommendations for

[172] David Banisar & Gus Hosein, *A Draft Commentary on the Council of Europe Cybercrime Convention* (Oct. 2002), http://privacy.openflows.org/pdf/coe_analysis.pdf, *archived at* http://perma.cc/5SNC-THQT.

[173] *See Google Transparency Report*, GOOGLE, https://docs.google.com/spreadsheets/d/1wt3DCBmG0Jp8YL6auFtSQJ9lCcGGZ61GKeosHRf0tLs/edit#gid=7453038 (last updated Sept. 23, 2015).

[174] *See Microsoft Law Enforcement Requests Report*, MICROSOFT, https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/lerr/, *archived at* https://perma.cc/6ULU-SC7F (last visited Dec. 3, 2015).

[175] *See Removal Requests*, TWITTER, https://transparency.twitter.com, *archived at* https://perma.cc/7RZN-77LD (last visited Oct. 1, 2015).

[176] *See Global Government Requests Report, January-June 2013*, FACEBOOK, https://www.facebook.com/about/government_requests, *archived at* https://perma.cc/Y6T4-UR7Q (last visited Oct. 1, 2015).

MLATS.[178] By 2010, the ICC was already involved in recommending technical standards for "best practices for lawful intercept requirements," including "dynamic triggering."[179] By 2012, it issued detailed recommendations for MLAT modifications.[180] The ICC refers to MLAT terms that enable and facilitate third party collaboration in LI as "benefits for governments, LEAs, and CSPs", and enumerates:

> • Consistent requirements can also help CSPs respond to LI requests in ways that accelerate access to data for LEAs, including by:
>
> ◊ Providing CSPs with clarity on LI requirements, which in turn reduces the real or perceived risk of subsequent legal challenge to a CSP decision to supply data and avoids the need for complex dialogues on legal requirements and processes; and
>
> ◊ Allowing CSPs to ensure that they have requisite legal authority to implement existing technical protocols for cross-border LI, such as the proposed European Telecommunications Standards Institute (ETSI) "dynamic triggering" process for mobile wiretaps.[181]

---

[177] Investopedia describes the International Chamber of Commerce (ICC) as the "largest, and arguably most diverse, business organization in the world with thousands of member companies representing over 130 countries and a vast array of business interests." *International Chamber of Commerce-ICC*, INVESTOPEDIA, http://www.investopedia.com/terms/i/international-chamber-of-commerce-icc.asp, *archived at* http://perma.cc/2MAY-XSLT (last visited Oct. 1, 2015).

[178] INT'L CHAMBER OF COMMERCE COMM'M ON THE DIGITAL ECON., TASK FORCE ON INTERNET AND TELECOMS, USING MUTUAL LEGAL ASSISTANCE TREATIES (MLATS) TO IMPROVE CROSS-BORDER LAWFUL INTERCEPT PROCEDURES, Doc. No. 373/512 (Dec. 9, 2012), http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/mlat/, *archived at* http://perma.cc/W73B-3SXF [hereinafter POL'Y STATEMENT OF 2012].

[179] *Id.* at 2, 5.

[180] *Id.*

[181] *Id.* at 5.

[75] The ICC acknowledges the risks to privacy, and gives a nod to individual rights, observing: "new processes for transferring personal information can raise tensions with privacy and data protection rights under national and transnational law. Both concerns are extremely important, and can be managed in a responsible manner."[182] However, few ideas are proposed for effectively protecting those rights.

[76] In 2010, the ICC recommended member countries adopt internationally consistent technical standards for LI.[183] Later, it noted that adoption and implementation of ETSI DTS 102 677 "could be influential" in ensuring CSPs "have the requisite legal authority to implement existing [and proposed] technical protocols for cross-border LI."[184] The proposed ETSI DTS 102 677 standard is one of a large set of LI technical standards for CSPs, which detail technically how surveillance works.[185] ETSI TS 187 005 provides further technical detail about how CSPs actually pick up our communications.[186]

[77] Facebook, Google, and other third parties work through the trade organization ICC to implement international surveillance technology standards.[187] The multi-stakeholder group Global Network Initiative—in

---

[182] POL'Y STATEMENT 2012, *supra* note 178, at 6.

[183] INT'L CHAMBER OF COM., COMM'N ON E-BUS., IT AND TELECOMS, TASK FORCE ON INTERNET AND TELECOMS INFRASTRUCTURE AND SERV'S (ITIS), GLOBAL BUS. RECOMMENDATIONS AND BEST PRACTICES FOR LAWFUL INTERCEPT REQUIREMENTS 1, 6–7 (2010), http://www.iccindiaonline.org/policy-statement/2.pdf, *archived at* http://perma.cc/L53G-9WSW.

[184] POL'Y STATEMENT OF 2012, *supra* note 178, at 5.

[185] *ESTI DTS 102 677*, *supra* note 165, at 7.

[186] *ETSI DTS 187 005*, *supra* note 169.

[187] GLOBAL NETWORK INITIATIVE, https://www.globalnetworkinitiative.org, http://globalnetworkinitiative.org/participants/index.php?qt-gni_participants=1#qt-

which Google and Microsoft, as well as other CSPs, participate—announced in its 2015 public policy agenda: "Data Beyond Borders: Mutual Legal Assistance in the Internet Era," setting forth a public policy agenda to help further shape MLAT policy.[188]

[78] A critical concept reflected in these documents is dynamic triggering.[189] ETSI TS 102 677 defines dynamic triggering as "a framework and architecture for achieving dynamic invocation of [Content of Communication (CC)]."[190] In other words, global CSP through ICC are recommending standards to accomplish interception, not just of metadata like time of communications and parties' names, but of the communications themselves. ETSI TS 102 677 goes on to state that its protocols are intended

> to be re-usable in any generic service domain and transport network scenario requiring the use of dynamic activation of lawful interception. The framework and architecture in the present document when included within specific service domain standards (e.g. 3GPP IMS) and transport network standards provides a consistent and inter-operable approach to dynamic triggering across multiple technology standards and/or multiple operators. The present document enhances other LI specifications to provide interoperability across different technologies or domains.[191]

[79] The role of MLATs in this otherwise dry technical standard

---

gni_participants, *archived at* http://perma.cc/WD8R-44TU (last visited Oct. 1, 2015).

[188] GLOBAL NETWORK INITIATIVE, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET ERA 2 (2015), https://globalnetworkinitiative.org/sites/default/files/GNI MLAT Report.pdf, *archived at* https://perma.cc/D76P-XY6A.

[189] *ETSI DTS 102 677*, *supra* note 165, at 11.

[190] *Id.* at 7.

[191] *Id.*

becomes clear: "[t]he present document assumes the necessary legal frameworks are in place to allow the use of dynamic triggering in both single and multiple operator domains. Any legal issues concerning the use of dynamic triggering are outside the scope of the present document."[192] In other words, technology can only accomplish so much. Beyond that, countries and individuals must seek a legal framework to justify surveillance.

III. MLATS AND CIVIL LIBERTIES

[80] As of 2013, the Supreme Court invalidated 176 laws as unconstitutional.[193] Against this background Google argues that secrecy laws surrounding surveillance themselves are illegal on the ground they violate the First Amendment.[194] One part of the government may abuse its ability to shape and pass laws that provide legal frameworks for agents' otherwise unlawful behavior. For example, treaties and laws that seek to allow what would otherwise be unlawful (or unconstitutional) intercept in the name of lawful intercept.

[81] MLAT's efforts to legalize reductions to civil liberties have also been pointed out by others. In 2004, Mark Rotenberg of EPIC[195] provided testimony to the U.S. Senate, presenting his work and the work of Gus Hosein at Privacy International and others on the Budapest Cybercrime

---

[192] *Id.*

[193] CONG. RESEARCH SERV., NO. 108-17, ACTS OF CONGRESS HELD UNCONSTITUTIONAL IN WHOLE OR IN PART BY THE SUPREME COURT OF THE UNITED STATES (2004), http://www.scribd.com/doc/88307065/Combined-Unconst-Acts, *archived at* http://perma.cc/FKU8-7J5J.

[194] *See, e.g.*, Julianne Pepitone, *Google Files First Amendment Court Case Against NSA Surveillance Secrecy*, CNN (June 18, 2013), http://money.cnn.com/2013/06/18/technology/security/google-nsa-first-amendment/, *archived at* http://perma.cc/SNY4-QUEP.

[195] EPIC Board & Staff, ELEC PRIVACY INFO. CTR. (last visited Oct. 30, 2015), https://epic.org/epic/staff_and_board.html, *archived at* https://perma.cc/6MZY-6PS8.

Treaty.[196] Rotenberg addressed four broad areas: that the treaty "[1] lacks adequate safeguards for privacy. . . [2] [has] vague and weak privacy protections. . . [3] [has] insufficient recognition of international human rights obligations. . . [and] [4] lacks a dual-criminality requirement."[197] He also noted that the work was "drafted in a secret and non-democratic manner," and "most European countries have failed to ratify" it.[198] Nevertheless, the U.S. did ratify the essentially unchanged treaty three years later—as did many other countries.[199]

[82] At this hearing, prior to the era of disclosures of mass surveillance, Rotenberg accurately foreshadowed the Snowden disclosures, stating:

> We object to the ratification of the Cybercrime Convention because it threatens core legal protections, in the United States Constitution, for persons in the United States. The treaty would create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards, and specifically lacking judicial review and probable cause determinations required under the Fourth Amendment. A significant number of provisions grant sweeping investigative powers of computer search and seizure and government surveillance of voice, e-mail, and data communications in the interests of law enforcement

[196] *See* CTR. FOR TECH. AND NAT'L SECURITY POL'Y, CROSSCUTTING ISSUES IN INT'L TRANSFORMATION (Dec. 2009), http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/What%20do%20Senior%20Leaders%20Need%20to%20Know%20About%20Cyberspace%20by%20Jeffrey%20Caton.pdf, *archived at* http://perma.cc/DJ5Y-395U.

[197] *See id.*

[198] *Id.* at 40–41.

[199] Michael A. Vatis, *The Council of Europe Convention on Cybercrime* at 209-10, *reprinted in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBER ATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY (2010), https://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf, *archived at* HTTPS://PERMA.CC/26T8-8ZZ2.

> agencies, but are not counterbalanced by accompanying protections of individual rights or limit on government use of these powers.[200]

[83] Two years earlier, Hosein and Banisar had warned similarly, "vague statements about the need to respect those rights . . . will quickly deteriorate in practice, to the lower common denominator."[201] Yet dire as the analyses of Rotenberg, Hosein, and Banisar were, the Department of Justice continues to draft MLATs further eroding civil liberties.

A. Judicial Review and Constitutional Supremacy

[84] In an amicus brief to *Boston College Trustees*, ACLU of Massachusetts (ACLUM) summarizes a key MLAT issue: "If the government has its way, its desired straightjacket on judicial review would apply to investigations and prosecutions by any foreign country party to an MLAT[.]"[202] The doctrine of judicial review and the supremacy of the Constitution enable access to all civil liberties protections and prevent the enforcement of unconstitutional laws. We briefly summarize judicial review here.

[85] The Constitution does not specifically use the term "judicial review." The power to declare laws unconstitutional is nevertheless a long-recognized aspect of the powers given to the Judiciary by Article III.[203]

[86] Essentially, since the Supremacy Clause says "[t]his Constitution" is the "supreme law of the land," federal statutes are lawful only when they emanate from the Constitution. State constitutions and statutes are

---

[200] *Hearing*, *supra* note 38, at 39.

[201] Banisar & Hosein, *supra* note 172, at 3.

[202] Br. for Ed Maloney, *supra* note 122, at 15.

[203] *See generally* Marbury v. Madison, 5 U.S. 137 (1803) (holding the court has power of judicial review).

valid only if they are consistent with the Constitution.[204] Any law contrary to the Constitution is unlawful. The Supreme Court has final jurisdiction in all cases arising under the Constitution, so it has the final authority to decide whether statutes are lawful—that is, consistent with the Constitution. This is how lawful Intercept (LI) can become Unlawful Intercept (ULI). Judicial review provides fundamental protection of civil liberties, and provides a check and balance of power on the Executive and Legislative, and branches.

[87] The Executive branch, having invested significant effort in negotiating MLATs, took the opportunity to expand its own powers and enable law enforcement goals to work around constitutional restrictions. It has worked continuously to convince the judicial branch of its lack of latitude to enforce constitutional protections. A review of Senate Foreign Relations Committee hearings regarding the Cayman Islands MLAT ironically reveals that leading conservative—and staunch opponent of the 1964 Civil Rights Act—Senator Jesse Helms as the main opponent of the Executive's strategy to reduce civil rights under MLATs.[205] He introduced a simple amendment: "To add an understanding that nothing in this treaty requires or authorizes legislation or other action by the United States of America prohibited by the Constitution of the United States."[206] Helms stated on October 24, 1989:

> I have insisted for months and months on end to the State Department that if clarifications such as I am offering today were incorporated into the MLAT's [*sic*], there would be no problem for me. But I took an oath right here on the floor, three times, to protect the constitutional rights of the American people. I do not intend to surrender those rights,

[204] *See* McCulloch v. Maryland, 17 U.S. 316, 406 (1819).

[205] 135 CONG. REC. S13,879–93 (daily ed. Oct 24, 1989) (statement of Sen. Helms).

[206] *Id.*

> even inadvertently.[207]

Helms addressed his remarks to none other than his distinguished colleague on the Committee, Senator John Kerry.[208] Kerry opposed Helms' opposition to ratifying the treaties and the two battled it out for two years.[209] Kerry stated in the same hearing, conceding Helms's point:

> Each of the treaties has an escape clause which permits our chief law enforcement official, the Attorney General, to make a determination, if at any time there is some reason to believe the treaties might be abused, that somehow the criminal justice process might be diverted by virtue of corrupt officials in another country or some other possible barrier to the appropriate use of these treaties, indeed the United States has the right not to provide information, not to cooperate under the treaty, as do other countries, similarly, if they think we are on a fishing expedition. . . . I understand wholeheartedly the interests that motivate the distinguished Senator from North Carolina. He has not sought changes in these treaties because he objects to the concept of cooperating or fighting the war on drugs. He has had legitimate concerns about the interests of the United States and the application of our own Constitution. I think those concerns have been met in the amendments we are poised to accept, and I want to thank the distinguished Senator for his cooperation in helping us to reach this point.[210]

[88] Helms' wording was eventually accepted in watered-down form.

---

[207] *Id.*

[208] *Id.*

[209] NADELMANN, *supra* note 114, at 383.

[210] 135 CONG. REC., *supra* note 206.

Curiously, no courts have reviewed Helms' extensive remarks in 1988-1989 insisting on these protections, Kerry's objections, or the clear intent of the ultimate adoption of constitutional supremacy. Instead, the courts over the past 30 years have tended to accept the Justice Department's assertion that performance is mandatory, and judicial review is precluded.

[89] Recently, however, courts have begun to reassert responsibility for judicial review of MLAT requests, citing separation of powers and the supremacy of the constitution.[211] Cases increasingly reflect this struggle, and seems headed to the Supreme Court for review. The Executive Branch continues to fight back on efforts to assert judicial discretion through government appeals.

[90] Recent cases winding their way through the courts appear to be starting to slowly confront the fundamental constitutional challenges of MLATs. In 2011, the Ninth Circuit issued a ruling that—while it did not benefit its hapless subject, Arkadi Gontmakher—did first seem to confront the issue of judicial review.[212] That case established that MLATs are subject to judicial discretion, albeit on a very limited basis.[213] This built on a similar Eleventh Circuit holding from 2003, which we review in the Law of the Requested State section.[214]

[91] Nevertheless, these rulings have been echoed in *Trustees of Boston College*, *Palmat*, and others to support the view that the executive branch espouses—that MLATs are subject to little or no judicial review.[215]

---

[211] United States v. Global Fishing (*In re* 840 140th Ave. NE), 634 F.3d 557, 567–68 (9th Cir. 2011).

[212] *See id.*

[213] *See id.* at 572.

[214] *See In re* Comm'r's Subpoenas, 325 F.3d 1287 (11th Cir. 2003); *infra* Part III.C.

[215] United States v. Trs. of Bos. Coll., 831 F. Supp. 2d 435 (D. Mass 2011) (recognizing that the Executive's interpretation of treaties are entitled to great weight); Palmat Int'l,

The ACLU of Massachusetts argued in its amicus brief to *Boston College Trustees* that "[t]hese cases effectively surrendered judicial review of foreign requests for evidence in criminal cases to the judgment of the executive branch. Nothing in the UK-MLAT requires such a result."[216] A review of these cases reveals the struggle between the executive and judicial branches ripe for Supreme Court review.

[92] The *Global Fishing* decision—increasingly cited and roundly criticized by the ACLU—states

> [o]ur conclusion that the parties to the treaty intended to remove the district court's traditional 'broad discretion' does not end the inquiry. The government argues that, upon receiving an MLAT request for assistance from the executive branch, the district court has no choice but to comply with that request." According to the government, the constitution imposes no limits on what the executive branch may require the courts to do in that situation.[217]

[93] We disagree. Treaties, like statutes, are subject to constitutional limits, including the separation of powers and the guarantee of due process.[218]

[94] The court goes on to say "[t]he enforcement of a subpoena is an

---

Inc. v. Holder, No. 12-20229, 2013 U.S. Dist. LEXIS 2004, at *9 (S.D. Fla. Feb. 14, 2013).

[216] Br. for Ed Maloney, *supra* note 122, at 21.
[217] *Id.*

[218] *See id.* at 571–72 (9th Cir. 2011) (citing Am. Ins. Ass'n v. Garamendi, 539 U.S. 396, 416, n. 9 (2003) (holding that treaties are "[s]ubject to the Constitution's guarantees of individual rights"); c*f. United Kingdom*, 870 F.2d at 693 n.8 (holding that in the context of a § 1782 request, that "[t]he district court's discretion is of course subject to the U.S. Constitution")).

exercise of judicial power."[219] It harshly criticizes the government's position, stating:

> According to the government, the executive branch has the authority to exercise that power directly, because the district court is required, by virtue of an MLAT request, to compel the production of requested documents. The government's position leads to the inescapable and unacceptable conclusion that the executive branch, and not the judicial branch, would exercise judicial power. Alternatively, the government's position suggests that by ratifying an MLAT, the legislative branch could compel the judicial branch to reach a particular result—issuing orders compelling production and denying motions for protective orders—in particular cases, notwithstanding any concerns—such as violations of individual rights—that a federal court may have. This too would be unacceptable.[220]

[95] Rulings since *Global Fishing* have picked up on the Ninth Circuit's nod to judicial accountability to the constitution, and the executive branch's opposition. Recently, the First Circuit widened the crack, opened by the Ninth Circuit, in MLATs' apparently impenetrable armor by asserting its right to judicial review, but declining to exercise it.[221] In 2013, the First Circuit also found that federal courts have the authority to quash MLAT subpoenas, but it declined to do so.[222]

[96] Between 2000 and 2006, Boston College academics carried out a project to record oral histories relating to armed domestic strife in Ireland

[219] *Id.* at 572.

[220] *Id.*

[221] *See In re* Price, 685 F.3d at 13.

[222] *See* United Kingdom v. Trs. of Bos. Coll., 718 F.3d 13, 22 (1st Cir. 2013).

in the 1970s between Ireland and the U.K.[223] A condition of the project was that Boston College would guard interviewees' confidentiality until their death, under what it believed and asserted to be an academic privilege conferred by the First Amendment.[224] Among those oral histories was testimony by former IRA members Brendan Hughes and Doulours Price regarding some alleged murders, including that in 1972 of Jean McConville, a widowed mother of 10 suspected of informing against the IRA.[225]

[97] In 2011, the U.K. filed a request for the recordings pursuant to its MLAT, which the U.S. Attorney General duly carried out, seeking and receiving in 2012 a subpoena directing Boston College to turn over the recordings.[226] They complied with the first subpoena as it included interviews with Brendan Hughes, a former Irish Republican Army (IRA) member who was by then deceased. However, in a second 2012 subpoena, Boston College was ordered to turn over 85 tapes—including that of the Doulours Price testimony—to Ireland.[227] Boston College appealed. It asserted, among other things, that revealing the contents of the recordings could expose Doulours Price and Boston College academics to acts of violent revenge.[228] In 2013, the First Circuit ruled against Boston College, ordering it to turn over additional recordings, including those of Doulours Price.[229] Thus, the court handed down a ruling against Boston College—a disappointment to First Amendment defenders in general, and those defending academic privilege in particular. The ruling did include a small

[223] *See id.* at 16–17.

[224] *See id.*

[225] *See id.* at 17–18.

[226] *See id.* at 18.

[227] *See Trs. of Bos. Coll.*, 718 F.3d at 18.

[228] *See id.*

[229] *See id.* at 27–28.

silver lining for concerned MLAT-watchers. It merely asserted that the doctrine of judicial review did not enable the DOJ to unilaterally force MLAT terms on the judiciary.[230] This came too late to help Doulours Price, as she was found dead in her home in January 2013.

> The First Circuit noted that Boston College
>
> > further urges this court to decide whether a district court has discretion to quash a subpoena issued pursuant to the US–UK MLAT. . . . The government, for its part, contends that courts do not have discretion under the US–UK MLAT to review for relevance materials subject to a subpoena. It states that only the Attorney General, not the courts, has discretion to decline, delay or narrow a request under the treaty . . . Pursuant to Article 3 of the US–UK MLAT, it is the Attorney General who decides whether to accede to a request from the UK, to narrow compliance to a certain aspect of said request or to decline to cooperate altogether.[231]

[98] The government, however, erroneously concludes that the Attorney General's exclusive prerogative in initiating proceedings translates into a general bar on judicial oversight of the subpoena enforcement process. The treaty is silent as to the role of federal courts in the process of enforcing subpoenas issued in furtherance of a request by the U.K. Of course, this silence does not mean that the actions taken by the Executive once the Attorney General decides to comply with a request are totally insulated and beyond the purview of oversight by the courts. In fact, courts play a prominent role in aiding the Executive's administration of its obligations under the treaty.[232] In *Boston College*, the First Circuit

[230] *See id.* at 21.

[231] *Id.* at 20–21.

[232] *See* 18 U.S.C. § 3512 (2012).

ruled that

> the enforcement of subpoenas is an inherent judicial function, which, by virtue of the doctrine of separation of powers, cannot be constitutionally divested from the courts of the United States. Nothing in the text of the US–UK MLAT, or its legislative history, has been cited by the government to lead us to conclude that the courts of the United States have been divested of an inherent judicial role that is basic to our function as judges.[233]

[99] The Court re-emphasizes this throughout the rest of the decision, noting it has "unequivocally established that courts have inherent judicial power over the enforcement of subpoenas issued in the context of a proceeding pursuant to the US–UK MLAT."[234] It expresses withering criticism of the government's position in footnote 5:

> On [one] occasion, the government assumed *arguendo* that the discretion to quash existed and that the court acted properly within it. . . .This is in sharp contrast to what the government had argued unsuccessfully in another case involving an MLAT where it denied such discretion existed.. . . In the appeal before us now, the government has again changed its position…and the guarantee of due process.[235]

[100] Thus, we see the executive branch continuing to pursue the argument that courts have no discretion over MLAT enforcement, and enforce the unconstitutional MLAT terms, while the judiciary begins to push back. Until the court awoke to the direct challenge to its own rights and authority, it seemed to take a laissez-faire attitude towards protecting

[233] *See Trs. of Bos. Coll.*, 718 F.3d at 23.

[234] *Id.*

[235] *Id.* at 21 n.5 (internal citations omitted).

the rights of individuals. Further MLAT challenges are likely to come before the courts.

[101] Following the decision against Boston College, the government was not satisfied to have prevailed over academic freedom. The government petitioned the judge to change his own *Boston College Trustees* ruling, to eliminate the very sections in which the court ventured its assertion of the separation of powers doctrine: "that federal courts have the authority to quash MLAT subpoenas."[236]

[102] "Relevant to this inquiry," Boston College's brief responds

> Boston College further urges this court to decide whether a district court has discretion to quash a subpoena issued pursuant to the US-UK MLAT. The government, for its part, contends that courts do not have discretion under the US-UK MLAT to review for relevance materials subject to a subpoena. It states that only the Attorney General, not the courts, has discretion to decline, delay or narrow a request under the treaty.[237]

[103] Boston College summarizes that the ruling

> accepted Boston College's argument that federal courts have authority to quash MLAT subpoenas, and . . . expressly rejected the government's argument that they did not. The government . . . did in fact address the issue, and did so in a contradictory fashion that, in the end, acknowledged federal courts' authority.[238]

---

[236] Opp'n of Bos. Coll. to Gov't's Pet. for Panel Reh'g at 2, United Kingdom v. Trs. of Bos. Coll. (*In re* Price), 718 F.3d 13 (1st Cir. 2013), http://lettersblogatory.com/wp-content/uploads/2013/09/gov.uscourts.ca1_.12-1236.00106573243.0.pdf, *archived at* http://perma.cc/WJ3J-8WRM.

[237] *See id.* at 6.

[238] *Id.* at 2.

[104] Boston College laid out its arguments for judicial review of MLATs, stating in "its responsive brief in this appeal, the government acknowledged that it had not appealed from the ruling below that the district court had authority to quash the US-UK MLAT subpoenas, explaining that the government 'was satisfied with the result reached by the district court.'"[239] Boston College continued that "the government nonetheless asserted in its responsive brief that the district court had no discretion to consider Boston College's objections to the subpoena under either the US-UK MLAT or 18 U.S.C. § 3512, and that the treaty 'reserves the authority to take these actions [to decline, delay, or narrow the request] to the Attorney General, not the *courts*. . . .'"[240] Boston College's brief quotes the government that "'[t]o the extent courts retain discretion,' that discretion should be narrowly exercised."[241] To support its argument, Boston College continues, "the government cited the same Ninth Circuit decision[*Global Fishing*], on which Boston College based its argument in the district court for that court's authority to quash MLAT subpoenas."[242]

[105] Boston College outlined its case for judicial review of MLATs, citing additional portions of the government's previously filed brief to show that the United States took a conflicting position regarding the court's authority to quash MLAT subpoenas earlier in the litigation than the position taken in the Petition for Rehearing. Boston College quotes that government brief as stating that while

---

[239] Opp'n of Bos. Coll. to Gov't's Pet. for Panel Reh'g, *supra* note 236, at 6. August 22, 2013 the First Circuit issued an errata sheet in response to the United States' August 2nd, 2013 Petition for Rehearing. Both parties briefed the issues raised by the United States' petition, and the court's errata amendments were incorporated in to the published opinion.

[240] *Id.* (parentheses and emphasis in original).

[241] *Id.*

[242] *Id.*

> this court was 'not require[d]' to address [the authority and scope of the federal courts' discretion in determining the legality of an MLAT subpoena] if it did so, 'it is the United States' position that the district court's discretion is limited to evaluating whether the issuance of a subpoena would offend some constitutional guarantee or violate a recognized federal privilege.[243]

Therefore, Boston College's brief continued,

> [i]t is puzzling that the government now seeks in its Petition for Rehearing a rewriting of this court's opinion to remove language confirming the authority of federal courts to quash MLAT subpoenas, when recognition of that authority is not substantially different from what the government in its responsive brief said is the 'United States' position' on the issue.[244]

[106] Boston College wryly observes, "[t]his court's decision apparently describes the nature of the courts' authority in more robust terms than the government likes. . . ."[245] Boston College concludes its arguments against expunging reference to judicial review of MLATs from the court's decision by invoking estoppel:

> The briefing history in this appeal shows that the government did have the opportunity to address, and actually did address, the issue of federal courts' authority to quash MLAT subpoenas. This history further shows that the government in its responsive brief did acknowledge that federal courts have 'discretion' – which presupposes

[243] *Id.* at 6–7.

[244] Opp'n of Bos. Coll. to Gov't's Pet. for Panel Reh'g, *supra* note 236, at 7.

[245] *Id.*

> authority – to quash MLAT subpoenas. This history requires rejection of the government's request now that the court rewrite its May 31, 2013 opinion to expunge the court's decision on this issue.[246]

[107] Judge Toruella agreed, and long after watchers had assumed the Boston College case was over, he issued another key ruling. He denied the government's request that the court essentially revise and expunge the portion of its own ruling, holding that MLAT subpoenas are subject to judicial review.[247] Thus, judicial review of MLAT subpoenas received recent support from the First Circuit, despite its overall adverse ruling on other civil liberties in *Boston College Trustees.*

[108] Rulings since *Boston College Trustees* have picked up this theme. *Palmat*, out of the Southern District of Florida notes the defendants base their claim in the Fifth and Fourteenth Amendment's protection of an individual's interests in avoiding the disclosure of personal matters.[248]

> For the reasons set forth below, the Court agrees with Petitioner's . . . argument . . . [that] the Supreme Court has observed, treaty obligations are 'subject... to the Constitution's guarantees of individual rights.. . .

---

[246] *Id.*

[247] Order Den. Reh'g, United States v. Trs. of Bos. Coll., No. 12-1236 (1st Cir. Sep. 5, 2013), https://bostoncollegesubpoena.wordpress.com/category/court-documents-and-exhibits/, *archived at* https://perma.cc/EE7P-SJXT.

[248] Order Granting Resp't Mot. to Dismiss, at 2–3, Palmat Int'l, Inc. v. Holder, No. 12-20229, 2013 U.S. Dist. LEXIS 2004, at *1 (S.D. Fla. Feb. 14, 2013) ("Palmat is a Florida corporation with its principal place of business in Florida. Wellisch is a foreign investor and Palmat's majority stockholder. In 2010, Argentina's Ministry of Foreign Affairs issued several requests to the U.S. Department of Justice for the production of Petitioners' financial records for bank accounts held in the United States. The requests were made as part of an ongoing criminal investigation stemming from allegations that Palmat, along with other companies, paid bribes to Argentine government officials in connection with the sale of agricultural equipment to the Venezuelan government.").

> .Therefore, the Court has federal question jurisdiction pursuant to 28 U.S.C. § 1331 over a claim that a treaty obligation does not comport with a constitutional guarantee.[249]

B. The Boomerang Effect: MLAT Collateral Impact

[109] Naturally, a hidden risk of MLATs involves the way they may boomerang back to harm citizens in countries normally enjoying constitutional protections to their civil liberties. In *US v. Trustees of Boston College*, [250] commentators appeared to miss this point. Conservatives who had never concerned themselves with the possible fallout of LEA-catering MLATs in the past expressed outrage when the UK enforced its US MLAT in the recent *US v. Trustees of Boston College* case. In a 2012 press release in New York, the Irish American Republicans (IAR) condemned "in the strongest terms []the actions of President Barack Obama and Attorney General Eric Holder in trying to take private property and invade the private research archives of an American university, and then turn them over to a foreign intelligence service."[251] It went on to lament, in new-found concern for the rights of the accused: "[t]he actions of the Obama administration are an utter disgrace, and a betrayal of the United States Bill of Rights and American national sovereignty."[252]

---

[249] *See* United States v. Moloney, (*In re* Price), 685 F.3d 1, 15 (1st Cir. 2012) (internal citation omitted) (exercising jurisdiction under 28 U.S.C. § 1331 to review an allegation that the petitioners' First Amendment rights would be violated based on a subpoena issued pursuant to an MLAT).

[250] *See generally* United Kingdom v. Trs. of Bos. Coll., 718 F.3d 13 (1st Cir. 2013) (failing to address MLATs).

[251] Press Release, Irish-American Republicans, IrishGOP Condems Obama/Holder MLAT Subpoena of Boston College (Feb. 2, 2012), https://bostoncollegesubpoena.wordpress.com/2012/02/02/irish-american-republicans-call-for-obamaholder-subpoena-to-be-quashed-in-irish-archives-boston-college-case/ *archived at* https://perma.cc/G48L-58Z3.

[252] *Id.*

[110] The IAR statement complained "Attorney General Holder had issued subpoenas to Boston College, directing the university to turn over its extensive research archives on the Irish Troubles to the intelligence services of the United Kingdom, 'a foreign nation.'"[253] Apparently ignorant of the compulsory nature of the US-UK MLATs,[254] the Obama administration, the statement said, "had *chosen* to act pursuant to the [MLAT] between the US and UK."[255] The First Circuit sided with the U.K. The release goes on to berate:

> The research archives of an American University are sacred, not to be delivered to foreign despots, by the government of the United States...Nothing could have a more chilling effect upon America's First Amendment rights to free speech, right to petition and due process, and the western tradition of academic freedom, then this cowardly stunt by the Obama administration to deliver a private American research archive to a foreign power. . . . We call upon the United States Court of Appeals, 1st Circuit, to uphold America's constitutional rights, and reject the subpoena to Boston College.[256]

[111] Another example of MLAT consequences unforeseen or unheeded when Congress approved them—as many would characterize *Boston*

---

[253] *Id.*

[254] Mutual Legal Assistance in Criminal Matters Treaty, U.S.-U.K., art. I, ¶ 2, Jan. 6, 1994, S. TREATY DOC. NO. 104-2 (1995), http://www.state.gov/documents/organization/176269.pdf, *archived at* http://perma.cc/WYW3-9XPP.

[255] Press Release, *supra* note 251.

[256] *Id.*

College—is this collateral damage to freedoms of US citizens.[257] *Global Fishing* illustrates this aspect of harm to US citizens from the MLAT's devil's bargain.[258] Russia was the actual party seeking action against a U.S. citizen in *Global Fishing*—it sought data regarding Arkadi Gontmakher, a Seattle businessman and U.S. citizen who was jailed and eventually tried in Russia on charges that he was involved in the illegal harvest and sale of king crab.[259] Gontmakher argued that Russia was on a fishing expedition; in other words, harassing him.[260] His pleading stated that "the Court should enter a protective order relieving Global [Fishing] of any obligation to produce documents for use in the Russian investigation."[261] They contended that the Russian proceedings are corrupt and illegal in a variety of ways, both in general and with respect to the specific proceedings against Gontmakher.[262] Apparently, there was credence to Gontmakher's protests, as he was eventually tried and acquitted in Russia, and "a Russian judge has ordered the Russian government to pay 100,000 rubles and apologize to [him]."[263]

[112] *Global Fishing* illustrates the lack of standing afforded defendants

---

[257] Sarah Cortes, *Legalizing Domestic Surveillance: The Role of Mutual Legal Assistance Treaties in Deanonymizing TorBrowser Technology* (unpublished manuscript) (on file with author).

[258] *Id.*

[259] *See* United States v. Global Fishing, Inc. (*In re* 840 140th Ave. NE), 634 F.3d 557, 561 (9th Cir. 2011).

[260] *Id.* at 563.

[261] *Id.* at 565.

[262] *Id.*

[263] Hal Bemton, *Judge: Russia Owes Bellevue Businessman Apology – and Rubles,* SEATTLE TIMES (Oct. 29, 2012), www.seattletimes.com/seattle-news/judge-russia-owes-bellevue-businessman-apology-8212-and-rubles/, *archived at* http://perma.cc/3MH8-7AU8.

under many U.S MLATs. However, it also illustrates a kind of banking against the Snowdens of the world—where the U.S may seek a return of the investment of helping Russia pursue its political enemies in return for cooperation in apprehending U.S.'s political enemies. Gonhtmakher, by all indications an innocent victim of Russian extortion, was calculated collateral damage, readily foreseeable when the treaty was drafted. By entering into its MLAT with Russia—stripped of civil liberties, especially in political cases—the U.S. seems to have effectively promised Russia that the U.S. DOJ will not blink at compulsory MLAT enforcement on behalf of Russia, even in Russian political cases against U.S. citizens. In return, we predict the U.S. will expect Russia to one day force Russian citizens/residents to comply with U.S. demands under the MLAT, when a Russian resident/citizen—like Snowden, for example—may be target of a possible U.S. government politically-inspired charge. It would seem that Snowden—now facing a possibly politically-inspired charge by the U.S. government, and possibly the death penalty, although now a Russian resident, two formerly disallowed conditions in MLATs—might fit this bill exactly.

C. MLATs and the Law of Requested States

[113] In 2003, a decision in a Eleventh Circuit case, *In re: Commissioner's Subpoenas*—an appeal from the U.S District Court for the Southern District of Florida—laid the groundwork for later erosion of civil liberties protections in MLATs.[264] The court held in reversing an order overruling MLAT compliance with a request from Canada regarding smuggling that "we reject appellee's argument that the 'law of the Requested State' should be read mechanically to incorporate all of the substantive law of the Requested State."[265] Deferring to the Executive Branch, the court in a single swipe knocked down the application of precedent to any MLAT treaty requests, sacrificing any protections in our own country and states in the service of ensuring cooperation with US

[264] *In re Comm'r's Subpoenas*, 325 F.3d at 1290.

[265] *Id.*

investigations and prosecutions in foreign countries. Referring to the Technical Analysis—or testimony regarding executive branch intent—the Court stated "The negotiator's explanation of [the treaty] . . . does not appear to support the appellees' reading."[266]

[114] The court noted that the treaty Technical Analysis "was prepared by the United States negotiating team, [and] constitutes the formal executive branch representations as to the meaning of this treaty and the obligations to be assumed by the United States under it."[267] "This official interpretation by the executive branch is entitled to great deference by this court," the court goes on to state, apparently less concerned with balancing deference to U.S constitutionality.[268] It then goes on to note that "the executive branch states that one purpose of . . . the MLAT, is to "provide[] slightly broader authority than 28 U.S.C. 1782 for U.S. federal courts to use their power to issue subpoenas and other process when Canada needs evidence for use before an administrative agency,"[269] sanctioning further expansion of Executive power, essentially granting it the ability to modify U.S. legislation when applying it in a treaty context.

[115] Carter-appointed Circuit Judge R. Lanier Anderson III wrote, "we conclude that the magistrate judge erred in construing the MLAT to express a clear and unambiguous intent to make requests under the Treaty subject to the limitations of all other substantive law of the United States[.]" Judge Anderson admitted, however, "undeniably, the magistrate judge's interpretation finds some support in the treaty text."[270]

D. MLATs and the Fifth, Sixth, and Fourteenth Amendments—Due Process is Not Applicable to Defendants

[266] *Id.* at 1297.

[267] *Id.* (internal citations omitted).

[268] *Id.* at 1298.

[269] *Id.*

[270] *Id.* at 1294.

[116] In many MLATs (notably U.S. MLATs) legal assistance through MLATs is not explicitly available to defendants.[271] For many years, and as recently as 2015, courts have held that individuals—in other words, defendants—have no right to enforce MLATs.[272] Others have questioned whether this exclusion is legal under the due process provisions of the Fifth, Sixth, and Fourteenth Amendments to the U.S. Constitution.[273]

[117] *United Kingdom v. United States* pitted the U.K. against the U.S. because the Crown Protection Service (CPS) "apparently pursuant to its discovery obligations under English law, served Appellants with a disclosure schedule prepared by the CPS and a British police constable after a visit to the offices of the US Secret Service in Miami."[274] In other words, the U.K. CPS recognized its obligation to assist defendants and attempted to use a MLAT on behalf of defendants. The U.S. denied the claim on the grounds it did not interpret the same MLAT to require the U.S. to recognize any such defendants' rights.[275]

[118] Alistair Brown notes that there exists the "apparent determination of some states at least to ensure that individuals cannot invoke treaty provisions. Again, this is most easily demonstrated under reference to

[271] *See, e.g.*, Agreement on Mutual Legal Assistance in Criminal Matters, U.S.-China, art. 1, June 19, 2000, T.I.O.S. No. 13102. The Agreement states, "[t]his Agreement is intended solely for mutual legal assistance between the Parties. The provisions of this Treaty shall not give rise to a right on the part of a private party to obtain, suppress or exclude any evidence or to impede the execution of a request."

[272] *See, e.g.*, United Kingdom v. United States, 238 F.3d 1312, 1317 (2001); *In re* Lavan, No. MISC-S-11-0019 GEB GGH, 2011 BL 76005, at *2, (E.D. Cal. Mar. 23, 2011).

[273] *See* David Whedbee, *Faint Shadow of the Sixth Amendment: Substantial Imbalance in Evidence-Gathering Capacity Abroad under the U.S.-P.R.C. Mutual Legal Assistance Agreement in Criminal Matters*, 12 PAC. RIM L. & POL'Y J. 561, 590 (2003).

[274] United Kingdom v. United States, 238 F.3d 1312, 1315 (2001).

[275] *See id.*

MLATs negotiated by the USA."[276] Brown notes

> It is accepted that it is open to the defence to enlist the aid of the court or even of the prosecutor in obtaining evidence under an MLAT but that is only half the story. In an adversarial system, the exclusion of evidence obtained irregularly is, if anything, more important to the defence in practice than obtaining evidence in support of a substantive defence on the merits.[277]

[119] MLAT partners have a wide variation in their respect for individual rights and freedoms, which may have inspired signatories to abandon their citizens' own rights and freedoms in the pursuit of law enforcement.[278] Foreign governments' ability to deprive U.S citizens of their rights through use of MLATs has increased. In its role as enforcer of foreign MLAT requests, the U.S actually acts on behalf of the foreign government in abridging U.S. citizens' rights.

E. MLATs and the Fifth Amendment: MLATs Have No Double Jeopardy Bar

[120] MLATs have long ignored the rights of individuals to access their provisions. Newer treaties remove protections routinely included in earlier MLATs, and further expand LEA scope. According to U.S Department of Justice documents, there are several benefits to MLATs over other types of treaties or legal tools.

[121] Brian Pearce, Resident Legal Adviser for the U.S. Embassy in Bangkok, points out in *Mutual Legal Assistance*, that "extradition treaties: double jeopardy is a bar (e.g., US-Thai Treaty Article 5: "If Requested State has tried fugitive for the same offense, extradition shall not be

[276] Brown, *supra* note 37, at 55.

[277] *Id.* at 56.

[278] *See id.* at 55.

granted.")[279] However, for "MLAT treaties: no such exception [exists]."[280] MLATs thus eliminate yet another right afforded under the Fifth Amendment's Due Process clause. In *United States v. Jeong*, a South Korean national was convicted in South Korea for paying bribes to American public officials. He was sentenced to time served—58 days plus an approximately $10,500 fine.[281] The U.S. then requested evidence under the U.S.-South Korean MLAT, which has no double jeopardy exclusion.[282] Nevertheless, the U.S. stated it was "not seeking to further prosecute Jeong," implying it would not put him in double jeopardy for the crime.[283] The defendant traveled to the U.S., believing he might receive assistance collecting money that his firm was owed by the agency he bribed.[284] Upon arrival in the U.S., he was promptly arrested and prosecuted for bribery, wire fraud, and conspiracy.[285] He was sentenced to five years and a $50,000 fine.[286] Apparently, the slap on the wrist imposed by South Korean judicial system did not seem to the DOJ OIA more than law enforcement theater. Jeong appealed on the grounds that the second prosecution violated the double jeopardy exclusion of another, multilateral MLAT.[287] The Fifth Circuit ruled against him, holding that no violation

[279] Brian Pearce, *Mutual Legal Assistance*, U.S. DEP'T OF JUSTICE, at 21, http://www.americanbar.org/content/dam/aba/directories/roli/raca/asia_raca_mlat_process.authcheckdam.pdf, *archived at* http://perma.cc/PRR4-VXMM.

[280] *Id.*

[281] *See* United States v. Jeong, 624 F.3d 706, 708–09 (5th Cir. 2010).

[282] *See* Treaty Between the United States of America and the Republic of Korea on Mutual Legal Assistance in Criminal Matters, U.S.-S. Kor., Nov. 23, 1993, S. TREATY DOC. NO. 104-1 (1995).

[283] *Jeong*, 624 F.3d at 712.

[284] *Id.* at 707.

[285] *Id.* at 709.

[286] *Id.* at 710.

[287] *See* Convention on Combating Bribery of Foreign Public Officials in International

occurred—neither of the bilateral nor the multilateral MLAT—and that double jeopardy does "not attach when separate sovereigns prosecute the same offense."[288]

[122] The U.S-South Korean MLAT—like most U.S. MLATs—omits any Fifth Amendment provision prohibiting double jeopardy.[289] Thus, the U.S. prosecuted Jeong twice for the same offense for which he was convicted in Korea, in a maneuver that would be unconstitutional by general Fifth Amendment standards—but perfectly permissible under the MLAT. When applying the MLAT to foreign nationals who admit to bribery—as Jeong did—this looks like a U.S law enforcement triumph for the public. The price is that U.S. citizens may be imprisoned and incarcerated abroad for offenses, for which they have already been tried in the U.S., including those for which they have been acquitted in a U.S. court.

F. MLATs and Dual Criminality

[123] Pearce highlights civil liberties rollbacks in other areas. He points out that "[t]here are several benefits to the MLAT process," noting that they, "often don't require dual criminality."[290] Indeed, a review of MLATs reveals that dual criminality requirements have quietly disappeared in recent treaties. For example, Article II, provision 3 of the 2009 US-Canada MLAT states "[a]ssistance shall be provided without regard to whether the conduct under investigation or prosecution in the Requesting State constitutes an offence or may be prosecuted by the Requested State."[291]

Business Transactions, U.S, Dec. 17, 1997, 105 U.S.T. 43 (ruling that Article 4.3, referring obliquely to double jeopardy, only required consultation, and then only upon request).

[288] *Jeong*, 624 F.3d at 712.

[289] *See id.*

[290] *See* Pearce, *supra* note 279, at 8.

[291] *See* Treaty Between the Government of Canada and the Government of the United

[124] But bars to Mutual Legal Assistance are now limited to military offenses, interference with investigation in the requested state, and tax offenses (under some treaties). This impact becomes clear when one considers the many countries with U.S. MLATs where anti-gay laws are enforced.[292] Eighteen of these countries have MLATs with the US.[293] By discarding longstanding dual criminality provisions, the many U.S. MLAT partners now have legal standing to pursue homosexuals, including demanding U.S. cooperation in their surveillance, apprehension, and extradition. Many other examples exist of laws in other countries that effectively criminalize otherwise law-abiding U.S. citizens.[294]

[125] The effects may be difficult to imagine, but include jailing U.S. citizens—or the citizens of U.S. allies—for homosexuality, assisted by

States of America on Mutual Legal Assistance in Criminal Matters, U.S.-Can., Mar. 18, 1985, Can. T.S. No. 19, http://www.oas.org/juridico/mla/en/traites/en_traites-mla-can-usa2.html, *archived at* http://perma.cc/S96J-W9PT [hereinafter US-Can. MLAT]; s*ee also* Treaty Between the Government of the United States and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, U.S.-Ir., Jan. 18, 2001, art. I, para. 3, http://www.state.gov/documents/organization/129536.pdf, *archived at* http://perma.cc/KQX4-SE3M [hereinafter US-Ir. MLAT].

[292] *See* Lucas Paoli Itaborahy & Jingshu Zhu, *State-Sponsored Homophobia, A World Survey of Laws: Criminalisation, Protection and Recognition of Same-Sex Love*, INT'L GAY BISEXUAL TRANS AND INTERSEX ASS'N (May 2013), http://old.ilga.org/Statehomophobia/ILGA_State_Sponsored_Homophobia_2013.pdf, *archived at* http://perma.cc/54ME-NYNR.

[293] *See id.* (listing countries with U.S. MLATs that criminalize homosexuality include Ukraine, Russia, Antigua & Barbuda, Barbados, Belize, Dominica, Grenada, Guyana, Jamaica, St. Kitts & Nevis, St. Lucia, St. Vincent & the Grenadines, Trinidad & Tobago, India, Malaysia, Morocco, Nigeria, and Egypt.).

[294] *See* David M. Herszenhorn, *New Russian Law Assesses Heavy Fines on Protesters*, N.Y. TIMES (June 8, 2012), http://www.nytimes.com/2012/06/09/world/europe/putin-signs-law-with-harsh-fines-for-protesters-in-russia.html?_r=0, *archived at* http://perma.cc/79D8-DJWN.

MLATs to enlist U.S. LEAs to gather evidence.[295] Further, they could be used to assist countries investigating their own nationals while in the U.S.

[126] Consider this scenario: your grandfather, a prominent academic in India comes to the U.S. as a visiting professor at Harvard for six months. He attends a rally protesting the election in India, where prominent gay rights activists also speak. India requests MLAT assistance from the U.S. LEAs—including Massachusetts State and the Harvard University police—seeking to prosecute him for the crime of homosexuality. Under the terms of the MLAT—into which the U.S. entered fully aware India has crimes on its books like this—the U.S. would have no choice but to assist in India's investigation of the professor, including possibly turning over any video of the professor at the rally.

G. MLATs and Political Offenses

[127] Initially, Nadelmann reports, exclusions for political offenses were included at Dutch insistence when negotiating that 1983 treaty,[296] much to the indignation of the Americans. "[W]hen obliged to negotiate such treaties with non-democratic governments because of broader concerns such as drug trafficking, U.S. negotiators typically insisted on including the 'political offense' exception clause."[297] However, they saw little need to include the clause in treaties with Western Europeans, particularly in MLATs. But "some European negotiators, including the Dutch, were less convinced that the clause should be excluded; they were influenced by their own perceptions of the conflicts between civil rights activists and law enforcement officials in the American South during the 1960's, and by

[295] *See* Kevin Rawlinson, *British Man Jailed for Four Months in Morocco 'for Being Gay'*, THE GUARDIAN, (Oct. 6, 2014, 7:53 AM), http://www.theguardian.com/world/2014/oct/06/british-man-ray-cole-70-jailed-four-months-morocco-gay, *archived at* http://perma.cc/57N9-Y9SD.

[296] NADELMANN, *supra* note 114, at 351.

[297] *Id.*

cases such as that involving the 'Chicago 7.'"[298] The American negotiators took umbrage at any suggestion that violations of U.S. laws—or prosecutions of criminal offenses—could be politically motivated or justified; they agreed, however, that insofar as extradition was deemed the most extreme form of international assistance in criminal cases, a political offense exception might be warranted in such treaties. However, they saw no need for its inclusion in the MLAT. When the Dutch insisted, the Americans relented.[299] It is worth noting that the Dutch treaty was second on the U.S. wish list, as Netherlands Antilles was considered to have the most stringent bank secrecy laws in the world, and thus was a primary haven for money launderers.[300]

[128] Pearce also highlights civil liberties rollbacks in other areas. He points out "Article 3 of US-Thai Treaty[provides]: 'Extradition shall not be granted' for political offense[s], military offense[s], or where 'extradition is requested for political purposes,'" however, "MLATs[] except military offenses, but generally don't exclude political offenses."[301] For example, the U.S.-Russia MLAT not only did not exclude political offenses;[302] it appends a note from the U.S. Embassy agreeing it has specifically omitted such during negotiations.[303] By contrast, the 1994 U.S.-U.K. MLAT[304]—used to subpoena the Boston College tapes—

[298] *Id.* at 352.

[299] *Id.*

[300] *Id.* at 349–50.

[301] Pearce, *supra* note 279, at 20.

[302] Treaty Between the United States of America and the Russian Federation on Mutual Legal Assistance in Criminal Matters, U.S.-Russ., June 17, 1999, S. TREATY DOC. NO. 106-22 (2002).

[303] *Id.* at 12.

[304] Treaty between the United States of America and the United Kingdom of Great Britain and Northern Ireland, U.S.-U.K., Jan. 6, 1994, S. TREATY DOC. NO. 104-2 (1996).

excludes assistance that "would be contrary to important public policy" or relating to "an offence of political character."[305] Interestingly, this MLAT was used to unjustifiably harass U.S. citizen Arkadi Gontmakher, and presumably under which the U.S. would in turn pursue assistance surveilling and prosecuting Edward Snowden.

[129] Some have asserted that the *In re* Price case is political.[306] According to the U.S.-U.K. MLAT, Mutual Legal Assistance is only available when the requesting country is "investigating conduct with a view to a criminal prosecution of the conduct, or referral of the conduct to criminal investigation or prosecution authorities, pursuant to its specific administrative or regulatory authority to undertake such investigation."[307] "Assistance shall not be available for matters in which the administrative authority anticipates that no prosecution or referral, as applicable, will take place," it states.[308]

[130] In 2014, the BBC reported that years earlier "187 people had received letters telling them they would not face prosecution for IRA crimes."[309] It then emerged that untold hundred had received Royal pardons for IRA activities.[310] In other words, it appeared the U.K.

[305] *Id.* at art. III ¶ 1(a), (c).

[306] *See* Br. for Ed Maloney, *supra* note 122, at 15.

[307] ESSENTIAL TEXTS ON INTERNATIONAL AND EUROPEAN CRIMINAL LAW 323 (Gert Vermeulen ed., 8th ed. 2012).

[308] 2 INT'L CRIM. L.: MULTILATERAL AND BILATERAL ENFORCEMENT MECHANISMS 486 (M. Cherif Bassiouni ed., 3rd ed. 2008).

[309] *John Downey Case 'has Implications for Northern Ireland Devolution'*, BBC (Feb. 26, 2014), http://www.bbc.com/news/uk-northern-ireland-26345267, *archived at* http://perma.cc/CV9D-GQTC.

[310] *See* Tom Whitehead, *Escaped IRA Terrorists Handed Royal Pardons as Part of Peace Deal, Queen had to Sign Off on Mercy Pardons that Allowed Convicted Killers and Fanatics to Return to Normal Lives*, THE TELEGRAPH, (Feb. 27, 2014), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10666040/Escaped-IRA-

government knew all along that it would never prosecute the Jean McConville murder, nor any other Belfast Project-related crimes, and so would never comply with the terms of the MLAT.[311] It then appeared that the real aim of the U.K.'s MLAT might have been solely political: raising the specter of 1972 crimes during an election season which included Sinn Fein leader Gerry Adams.[312] Adams was the one Brendan Hughes and Doulours Price identified as the one who ordered the murder of McConville and others.[313]

H. MLATs and Death Penalty Bars

[131] Pearce indicates "[e]xtradition treaties often provide there may be no extradition for offenses which are punishable by death in Requesting State, but not in Requested State (e.g., Article 6)."[314] But for "MLAT Treaties, no such limitation [exists],"[315] eliminating a right afforded under

terrorists-handed-Royal-pardons-as-part-of-peace-deal.html, *archived at* http://perma.cc/W4VD-9D3A; *see also* Chris Kilpatrick, *Stormont Crisis: Spotlight Falls on Pardons Granted by Queen to IRA Men Questions Being Asked Over any Other Deals Cut Behind Closed Doors*, BELFAST TELEGRAPH (Feb. 27, 2014), http://www.belfasttelegraph.co.uk/news/northern-ireland/stormont-crisis-spotlight-falls-on-pardons-granted-by-queen-to-ira-men-30046304.html, *archived at* http://perma.cc/S9XJ-Z5AV.

[311] *See* Conor Macauley, *Boston College Prepared to Return Troubles Tapes*, BBC (May 6, 2014), http://www.bbc.com/news/uk-northern-ireland-27286543, *archived at* http://perma.cc/TX6J-K35W.

[312] *See BC Archive Case Appears Politically Motivated*, THE IRISH ECHO (Oct. 12, 2011), http://irishecho.com/2011/10/bc-archive-case-appears-politically-motivated/, *archived at* http://perma.cc/S2SP-ZUMD.

[313] *See id.*

[314] Pearce, *supra* note 279, at 22.

[315] *Id.*

the Eighth Amendment.[316] Nineteen states outlaw the death penalty.[317] But U.S. MLAT drafters, reviewers, and approvers see fit to collaborate to facilitate investigation and prosecution in situations where the penalty in the requesting country will be terminal.

[132] For instance, "country surveys . . . indicate that apostasy laws are frequently used to charge persons for acts other than conversion. For example, in Mauritania, Saudi Arabia, Jordan, and Yemen, individuals were charged with apostasy for their writings or comments on social media." [318] Salman Rushdie and others were sought for criminal prosecution (and punishment by death) by the Iranian state for ostensibly criticizing Islam.[319] As another example, in many Islamic countries, laws require women to wear hijab.[320] Under the terms of this MLAT with Iran,[321] it appears India may have agreed to assist Iran in pursuing women

[316] U.S. CONST. amend. VIII.

[317] See *States With and Without the Death Penalty*, DEATH PENALTY INFO. CTR., http://www.deathpenaltyinfo.org/states-and-without-death-penalty, *archived at* http://perma.cc/4U62-BVWQ (last visited Dec. 3, 2015).

[318] *Id.*

[319] Barbara Crossette, *Iran Drops Rushdie Death Threat, And Britain Renews Teheran Ties*, N.Y. TIMES (Sept. 25, 1998), http://www.nytimes.com/books/99/04/18/secials/rushdie-drops.html, *archived at* http://perma.cc/8BGD-7RP3.

[320] *Islamic Penal Code of the Islamic Republic of Iran – Book Five, Chapter Eighteen, Article 638*, IRAN HUMAN RIGHTS DOC. CTR. (July 18, 2013), http://iranhrdc.org/english/human-rights-documents/iranian-codes/1000000351-islamic-penal-coe-of-the-islamic-republic-of-iran-book-five.html#18, *archived at* http://perma.cc/G964-YZ7F (explaining that a hijab is a full set of garments for women only, that can cover the entire body, including eyes, face, head, arms, hands, legs, and feet. Some states assert that a hijab is required under Islamic law, while others disagree. The Qu'ran does not explicitly require hijab, but includes an exhortation for women to cover themselves).

[321] GOV'T OF INDIA MINISTRY OF HOME AFFAIRS: POL'Y PLANNING DIV., http://mha.nic.in/Policy_Planing_Division, *archived at* http://perma.cc/7QJX-W34V (last

under its jurisdiction, not dressed according to Iran's tastes.

I. MLATs and Search, Seizure, and Online Surveillance

[133] We have reviewed MLATs' lack of Fifth, Sixth, Eight, and Fourteenth Amendment protections. The section on U.S. DOJ motivation to achieve MLAT performance certainly revolved around search and seizure, an area generally subject to Fourth Amendment protections. In its amicus brief in *Boston College Trustees*, the ACLUM summed up the issue: "ACLUM is concerned about the government's position in this case that governments who are parties to Mutual Law Assistance Treaties should have greater rights than United States federal and local law enforcement authorities to subpoena documents without judicial review."[322] This case reflected public outcry in the U.S.—particularly among Irish-Americans and friends of academic freedom—about the request by the U.K. to seize recordings of oral histories of IRA members.[323] The heart of that outcry concerned public realization and disbelief that MLATs lack Fourth Amendment protections, or that judicial review and relief regarding these protections is unavailable to them.

J. MLATs and Wiretapping

[134] The Wiretap Act bases its search and seizure protections in Fourth Amendment judicial review requirements and probable cause determinations.[324] Modern MLATs eliminate these obstacles for LEAs. By

visited Dec. 3, 2015) (stating "India has so far operationalised these Treaties with the following 34 countries […] Iran").

[322] Br. for Ed Maloney, *supra* note 122, at 7–8.

[323] United States v. Trs. of Bos. Coll., 831 F. Supp. 2d 435, 455 (D. Mass. 2011).

[324] *See, e.g.*, U.S. Patriot Act of 2001, 115 Stat. 272 (codified as amended in scattered sections of 18 U.S.C. § 1); Communications Assistance for Law Enforcement Act of 1994, 108 Stat. 4279 (codified as amended in scattered sections of 47 U.S.C. § 1001).

eliminating constitutional constraints on search and seizure—including that of personal data and communications under government surveillance—MLATs, when applied to Americans, expose them to an unfamiliar lack of civil liberties.

[135] In *United States v. Rommy,* the Second Circuit established that the United States government may conduct investigations (including surveillance) outside MLATs.[325] Pursuant to MLAT requests from the U.S. in 2002, "the Netherlands provided the United States with a transcript of a . . . call intercepted by the Dutch police in which Rommy and an unnamed confederate discussed the limited supplies of 'Versace t-shirts.'"[326] "Rommy contended that the DEA violated the MLAT in effect between the United States and the Netherlands—as well as Dutch domestic law—by employing a confidential informant (DeVries) to gather evidence in the Netherlands after Dutch officials had denied the United States' MLAT request to conduct an undercover investigation in their country."[327] The judge held an MLAT procedure is nice but not necessary, and denied the motion to reverse the ultimate conviction on this, and all other grounds.[328]

[136] In this case, the Dutch courts actually denied the first MLAT request for surveillance of Rommy for lack of probable cause.[329] In similar cases, when the legal shoe is on the U.S. foot, the U.S. Attorney General and U.S. Courts have claimed MLATs preclude such refusals.[330] Not to be

[325] *See* United States v. Rommy, 506 F.3d 108, 140 (2d Cir. 2007).

[326] *Id.* at 113.

[327] *Id.* at 128.

[328] *Id.* at 128–31.

[329] *Id.* at 113.

[330] *See, e.g.*, United States v. Moloney (*In re* Price), 685 F.3d 1, 11–14 (1st Cir. 2012) (holding that two subpoenas in an investigation of two academic researchers were not precluded from disclosure under MLAT); *see also* United States v. Under Seal (*In re*

deterred, the U.S. conducted its own investigation of Rommy in the Netherlands.[331] On the grounds of evidence thus gathered in disregard of the agreed-upon MLAT procedure, the Netherlands relented upon a second MLAT request from the U.S., and agreed to allow Rommy's surveillance.[332]

K. MLATs and FOIAs

[137] Even the FOIA has not survived MLATs. A report submitted to the Senate by Senator Jesse Helms on the Senate Foreign Relations Committee stated "[m]ost MLATs allow the Central Authorities of the country providing evidence or information under the Treaty to prohibit its use in other investigations, prosecutions, or proceedings without their consent. . . . In this country, the limitation places the MLAT information and evidence initially beyond the reach of a Freedom of Information Act request."[333]

L. MLAT and International Law

[138] Before reviewing surveillance and Fourth Amendment issues, we briefly review contraventions to international law. With respect to international privacy treaties and MLATs, we find a disconnect between MLAT treaty provisions and privacy protections in other treaties. For example, the 1966 U.N. International Covenant on Civil and Political Rights (ICCPR) and the 1953 COE European Convention on Human

Grand Jury Subpoena), 646 F.3d 159, 165 (4th Cir. 2011) (finding that MLAT did not give a private right of action to protect subpoenas, regarding documents in discovery between two companies, from government investigation).

[331] *See Rommy*, 506 F.3d at 113.

[332] *Id.*

[333] S. EXEC. REP. NO. 106-24, at 6 (2000), http://www.gpo.gov/fdsys/pkg/CRPT-106erpt24/pdf/CRPT-106erpt24.pdf, *archived at* http://perma.cc/5QS8-GLTB.

Rights (ECHR) are two treaties considered to bear on privacy internationally.[334] But their terms—like those of other treaties and laws—have never been applied to MLATs.

[139] The European Parliament noted in its 2014 report its disapprobation of U.S. stance that non-U.S. citizens may be accorded a sort of second-class status with respect to civil liberties accorded its own citizens, as in MLATs:

> [I]n respect of intelligence activities concerning non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognise the fundamental principle of respect for privacy and human dignity as enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights . . . whereas we find [the U.S. government] does not recommend granting non-US persons the same rights and protections as US persons.[335]

The report also notes the threat U.S. mass surveillance poses. It states:

> these risks [to liberty] do not only originate in criminal activities (against which the EU legislator has adopted a series of instruments) or from possible cyber attacks from governments of countries with a lower democratic record.

---

[334] 1953 Council of Europe's European Convention on Human Rights (ECHR), art. 8, http://www.echr.coe.int/Documents/Convention_ENG.pdf, *archived at* http://perma.cc/8T7N-EK9U; 1966 U.N. International Covenant on Civil and Political Rights (ICCPR), art. 17, https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf, *archived at* https://perma.cc/67U4-SG78.

[335] *Report on the U.S. NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs*, at 10 (Feb. 21, 2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN, http://perma.cc/3GSW-G7X3.

> There is a realization that such risks may also come from law enforcement and intelligence services of democratic countries putting E.U. citizens or companies under conflicts of laws resulting in a lesser legal certainty, with possible violations of rights without proper redress mechanisms.[336]

[140] With respect to MLATs, the report observes their recognized role in acquiring information:

> Calls on the Commission to conduct . . . an in-depth assessment of the existing Mutual Legal Assistance Agreement . . . in order to verify its practical implementation and, in particular, whether the US has made effective use of it for obtaining information or evidence in the EU and whether the Agreement has been circumvented to acquire the information directly in the EU, and to assess the impact on the fundamental rights of individuals; such an assessment should not only refer to US official statements as a sufficient basis for the analysis but also be based on specific EU evaluations.[337]

Finally, specific privacy protections in MLATs are few and far between, and precede the modern era of digital communications. For example, Article 26 of the E.U. MLAC refers to data protection.[338] However, the protections there are vague, especially compared with the provisions for LEAs. In conclusion, U.S. citizens and others seem to have been deprived of a full range of civil liberties through Executive Branch action, through what it maintains is compulsory international treaty reflexivity.

---

[336] *Id.* at 4.

[337] *Id.* at 28.

[338] *See* EU MLAC, *supra* note 145, at art. 13.

IV. MLATs AND LEGAL FRAMEWORKS FOR SURVEILLANCE

[141] Mutual Legal Assistance is certainly a critical element to a civil society, as is surveillance. Victims and targets of crime will be the first to seek to take advantage of MLAT capabilities, and will demand that law enforcement worldwide spare no effort to investigate, survey, apprehend, and arrest criminals. Certainly MLATs and surveillance have a legitimate role to play as a tool to improve law enforcement—no less, of course, than do privacy- and anonymity-protecting MJAT tools like Tor Browser, extensively used by law enforcement. Yet laws and legal tools that fail to replicate privacy and other civil protections can cause harm, as well as reduce security. MLATs create legal frameworks that can be used to justify surveillance that is otherwise Unlawful Intercept. We briefly review case law, including very recent cases that have upheld these legal frameworks. We use the term Unlawful Intercept ("ULI")—meaning unconstitutional surveillance—to contrast with Lawful Intercept ("LI"), itself a synonym for government surveillance.

A. MLAT Explicit References to Surveillance

[142] We have reviewed numerous treaties in Section Two that explicitly incorporate reference to telecommunications and data surveillance with weak safeguards, or where drafters testified that this was their intent. As we have seen in *In re Commissioner's Subpoenas*—the Canadian smuggling case—not only the explicit treaty provisions, but also their intent forms the legal basis for later review in the courts.[339] We recall Judge Anderson's words: "The negotiators' explanation of [the treaty], provided in the Technical Analysis, does not support the appellees' reading."[340]

[143] The U.S. Senate hearing testimony by Mary Ellen Warlow—the Director of the Office Of International Affairs, Criminal Division, U.S. Department of Justice—explains how the desire for legal justification for

[339] *See generally In re* Comm'r's Subpoenas, 325 F.3d 1287 (11th Cir. 2003).
[340] *Id.* at 1297.

surveillance motivated not only the U.S., but also Germany in drafting recent MLATs. She said "this is the first United States MLAT to include . . . telecommunications surveillance. . . . This provision was included at Germany's request, to assert the Federal government's legal authority, vis-à-vis the States, to undertake such actions on behalf of foreign authorities." [341] The testimony of Samuel M. Witten—Deputy Legal Adviser for the U.S. Department Of State—further established intent, by saying "[t]he proposed U.S.-Germany Mutual Legal Assistance Treaty in Criminal Matters (MLAT). . . has several innovations, including telecommunications surveillance[.]"[342]

[144] We have already reviewed detailed surveillance provisions in specific treaties in Section Two. We now review how other MLAT provisions add to the legal basis for surveillance.

B. Spontaneous Information

[145] "The US National Security Agency circumvents UK law by offering, rather than being asked for, intelligence from global websites to their British counterparts, according to David Blunkett, who was home secretary at the time of the 9/11 attacks," according to a 2013 report by the Guardian, which further states ". . .Blunkett highlighted one of the key areas at the heart of investigations into whether Britain's GCHQ

[341] *Concerning Law Enforcement Treaties: Hearing on Law Enforcement Treaties Before the S. Comm. on Foreign Relations,* 109th Cong. 10, (2005) (statement by Mary Ellen Warlow, Director, Office of Int'l Affairs, Dep't of Justice), http://www.state.gov/documents/organization/87297.pdf, *archived at* http://perma.cc/462C-PJ3P.

[342] *On an Extradition Treaty with Great Britain and Northern Ireland, an Extradition Protocol with Israel, a Mutual Legal Assistance Treaty with Germany, and a Mutual Legal Assistance Treaty with Japan: Hearing on Law Enforcement Treaties Before the S. Comm.oOn Foreign Relations, 109th Cong.* 10, (2005) (statement by Samuel M. Witten, Deputy Legal Adviser, U.S. Dep't Of State), http://www.state.gov/s/l/2005/87190.htm, *archived at* http://perma.cc/LQ9M-5L7.

eavesdropping centre has abided by the law."[343] Exactly what law, however, was not clear. However, an examination of the Budapest Cybercrime Treaty may finally clear up this question. That treaty enshrines in law the idea that countries just help each other out, unsolicited:

> A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for cooperation by that Party under this chapter.[344]

[146] According to Article 26, the provision appears to be custom-made to fit into the US "international silver platter doctrine,"[345] which courts have been using to uphold what would otherwise amount to violations of the Fourth Amendment. The Budapest Cybercrime Treaty states:

---

[343] Nicholas Watt, *NSA 'offers intelligence to British counterparts to skirt UK law'*, THE GUARDIAN (June 10, 2013), http://www.theguardian.com/politics/2013/jun/10/nsa-offers-intelligence-british-counterparts-blunkett, *archived at* http://perma.cc/W3FK-VCKW.

[344] *Budapest Cybercrime Treaty*, *supra* note 75, at art. 26.

[345] International silver platter doctrine, which holds that allowed evidence seized illegally by agents other than U.S. Federal agents, i.e. foreign law enforcement, may be admitted in U.S. federal court as long as the foreign officials were not acting as agents of federal law enforcement. The court reasons that foreign agents are not deterred by the exclusionary rule, and evidence handed to U.S. federal agents "on a silver platter" may be admitted. This theory was discredited and thrown out after 50 years of misuse in the US courts pertaining to evidence obtained illegally by domestic police, i.e. state and local police. Yet it lives on as a Fourth Amendment exception for foreign police evidence. *See* Lustig v. United States, 338 U.S. 74, 78–79 (1949) (plurality opinion).

> Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.[346]

[147] This provision sounds highly familiar. It is in fact a review of parallel construction,[347] with its imperative to keep the real source of information—unlawful surveillance—a secret. We discuss the Silver Platter Doctrine after a review of JITs.

C. JITs and Collaborative Surveillance

[148] The EU MLAC first provided for Joint Investigative Task Forces (JITs) in 2000.[348] JITs bring together members of law enforcement from

[346] *Budapest Cybercrime Treaty*, *supra* note 75.

[347] *See* Shiffman & Cooke, *supra* note 49.

[348] *See, e.g.*, EU MLAC, *supra* note 145, at art. 13; *see also Summaries of E.U. legislation – Mutual assistance in criminal matters between Member States*, EUR-LEX EUROPA, http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/l33108_en.htm, *archived at* http://perma.cc/75X6-BTXA (last updated Dec. 20, 2011). JITs originate in more than one source. We cite the principal sources, without going further into the history. Europol, the European Union Police Alliance website also provides background. *General Legal Basis for JITs*, EUROPOL, https://www.europol.europa.eu/content/general-legal-basis-jits, *archived at* https://perma.cc/4VHW-NT3B ("Joint Investigation Teams [are] provided for in Article 13 of the 2000 MLA Convention.") (last visited Dec. 3. 2015); E.U.-U.S. MLAT, *supra* note 75, at art. 5. While established in the 2000 Act, JITs did not actually commence until 2005. Thus, the E.U.-U.S. MLAT can also be considered to be the origination point for JITs. Confusingly, this treaty did not enter into force (EIF) until 2010. Its drafting, signing, ratification and entry into force spanned seven years, which is not unusual for treaties. Thus, while its initial draft preceded the actual formation of JITs in 2005, and thus can be considered the origin of JITs, its final EIF followed that of the E.U. MLAC.

multiple countries. Article 13, Provision 7 states:

> Where the joint investigation team needs investigative measures to be taken in one of the Member States setting up the team, members seconded to the team by that Member State may request their own competent authorities to take those measures. Those measures shall be considered in that Member State under the conditions which would apply if they were requested in a national investigation.[349]

[149] Thus, for example, if a U.S. LEA is the originating Member State, it can request to set up a JIT in France, with members "seconded" from France, Croatia, Bulgaria, and Jamaica. Thus, a U.S. case can become a French, Croatian, Bulgarian, and Jamaican case. When the U.S. ultimately seeks surveillance data about a U.S. citizen in Jamaica, that would under U.S. law be prohibited domestic surveillance. However, once it forms a JIT with Jamaica, it also becomes a Jamaican case. In seeking surveillance data about a U.S. citizen, Jamaica is free to surveil the U.S. national as a foreign citizen. The JIT then allows Jamaica to share the resulting surveillance with the rest of the JIT members, including the U.S. LEA. E.U. MLAC Provision 9 states:

> A member of the joint investigation team may, in accordance with his or her national law and within the limits of his or her competence, provide the team with information available in the Member State which has seconded him or her for the purpose of the criminal investigations conducted by the team.[350]

[150] JITs come to mind when reflecting on The Guardian's report from 2013, that reports "[t]he US National Security Agency circumvents UK law by offering, rather than being asked for, intelligence from global

[349] EU MLAC, *supra* note 145, at art. 13, para. 7.

[350] *Id.* at art. 13, para. 9.

websites to their British counterparts, according to David Blunkett."[351] In this way, MLAT JITs facilitate cooperative surveillance by collaborating governments. In other words, they legalize formerly Unlawful Intercepts.

In *Getto I*, the court held

> ongoing collaboration between an American law enforcement agency and its foreign counterpart in the course of parallel investigations does not—without American control, direction, or an intent to evade the Constitution—give rise to a relationship between the two entities sufficient to apply the exclusionary rule to evidence obtained abroad by foreign law enforcement.[352]

[152] The Court also held "the alleged warrantless searches and surveillance do not shock the judicial conscience."[353] What *does* shock the conscience is that—considering of the facts of the investigation—the Court could have found an absence of "American control, direction, or an intent to evade the Constitution."[354]

D. International Silver Platter Doctrine

[153] The Silver Platter doctrine fits precisely into the Spontaneous-cooperation clause of the Budapest Cybercrime Treaty and into the JIT provisions of that and most other modern MLATs. In 2014, the Second Circuit issued its second and final ruling in *United States v. Getto*.[355]

[351] Watt, *supra* note 343.

[352] United States v. Getto (*Getto I*), 729 F.3d 221, 224 (2d Cir. 2013).

[353] *Id.*

[354] *Id.*

[355] United States v. Getto (*Getto II*), 586 Fed. App'x 11, 13 (2d Cir. 2014).

There, the court demonstrated its determination to turn a blind eye to the reality of U.S. MLAT influence over foreign LEAs and the example it sets in the world by upholding the admissibility of evidence—specifically, surveillance—legally gathered under MLATs, despite court findings that the evidence was gathered illegally by many other standards.[356] In *Getto I*, an American citizen appealed his conviction in a case involving surveillance of a "lottery telemarketing scheme operated out of three so-called 'boiler rooms'" in Israel.[357] The court insisted that Israeli LEAs are not agents of U.S. LEAs.[358] This reasoning is echoed in the decision in *United States v. Lee*, when U.S. LEA purchased surveillance equipment for a Jamaican LEA, provided their training in its use, and in other ways might have been seen to have "directed" the operation.[359] This might violate U.S. law prohibiting seeking methods "designed to evade constitutional requirements."[360]

[154] Not so, found Judge José A. Cabranes of the Second Circuit, the judge in both cases. U.S. LEAs did not "direct" searches and seizures in these cases.[361] In contrast with the finding in *Elkins v. United States* that ended the domestic silver platter exception to the Fourth Amendment,[362] Cabranes' rulings appear to demonstrate that over 50 years later—despite it being a different world where crime is internationalized—U.S. judges are not prepared to acknowledge constitutional evasion maneuvers called out years before by their colleagues. The court "reason[ed] that 'the mere

[356] *Id.*

[357] *Getto I*, 729 F.3d at 225.

[358] *Id.* at 230–31.

[359] United States v. Lee, 723 F.3d 134, 141 (2d Cir. 2013).

[360] *Id.* at 140.

[361] *Id.* at 139.

[362] *Id.* at 139 n. 3 (distinguishing domestic silver platter with international silver platter doctrine).

fact that an [MLAT] existed, information was shared and the DEA provided money, training and [surveillance] equipment does not warrant a finding of agency' between the DEA and Jamaican law enforcement."[363] The court found "the two nations signed a Memorandum of Understanding ("MOU") in 2004 to establish a program in which Jamaican law enforcement officers, *inter alia*, 'would monitor intercepted phone conversations authorized by Jamaican court orders for purposes of both countries gathering evidence or leads to obtain evidence in narcotics investigations.'"[364]

[155] In *Getto I*, the court held that Israeli LEAs are not acting as "agents" of U.S. LEAs, even when the U.S. LEA purchased surveillance equipment for the foreign LEA and, as in *United States v. Lee*, provided their training in its use, and in other ways directed the investigation.[365] Getto pointed out that "(1) the INP initiated its investigation based on the MLAT request from American law enforcement officials; (2) Israel never sought to prosecute Getto; (3) many other members of the conspiracy, or related conspiracies, were extradited to the United States; and (4) an article in an Israeli newspaper stated that American law enforcement agents watched live surveillance of the Ha'Negev boiler room."[366] The court found that "the MLAT request, the information-sharing between American law enforcement and the INP, and American receipt of the fruits of the INP's investigation in Israel – reveals no cooperation 'designed to evade constitutional requirements.'"]Thus, it reasoned that the evidence need not be excluded, and upheld Getto's conviction.[367] The court found that Israeli LEAs are not acting as agents of U.S. LEAs, despite

[363] *Id.* at 138.

[364] *Lee*, 723 F.3d at 137.

[365] *Getto I*, 729 F.3d at 231.

[366] *Id.* at 230.

[367] *Id.* at 234–35.

appearances to the contrary.[368] Getto also asserted the Israeli National Police acted as agents under the joint venture doctrine, a doctrine which the Second Circuit does not recognize and explicitly declined to adopt in this case.[369]

E. JITs and the European Parliament

[156] Regarding JITs, the European Parliament reported as a result of its investigation [370] that "the revelations since June 2013 have caused numerous concerns within the EU as to. . .

> the degree of cooperation and involvement of certain EU Member States with US surveillance programmes or equivalent programmes at national level as unveiled by the media; the lack of control and effective oversight by the US political authorities and certain EU Member States over their intelligence communities; the possibility of these mass surveillance operations being used for reasons other than national security and the fight against terrorism in the strict sense, for example economic and industrial espionage or profiling on political grounds; . . . the respective roles and degree of involvement of intelligence agencies and private IT and telecom companies; the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect

[368] *Id.* at 230–32.

[369] *Id.*

[370] EU Comm. on Civil Liberties, Justice and Home Affairs, *European Parliament Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,* art. F (2013), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN, *archived at* http://perma.cc/A7BN-GE7M.

> and being subject to surveillance[.][371]

[157] Reuters first reported the concept of parallel construction in 2013.[372] It is a short step from using JIT cooperative surveillance to using JITs to facilitate legal window dressing for parallel construction.

F. Value of Measuring MLATs and Lawful Intercept in an Era of Unlawful Intercept

[158] We now briefly pause to examine the value of LI indicators in an era of covert mass global surveillance. Given revelations that GIAs around the world perform surveillance unconstrained by laws, is there anything to learn from analyzing the indicia of each country's LI propensity, such as MLATs?

[159] The nature of government surveillance is covert. By contrast, it would seem MLATs are overt (albeit very low profile) tools, which may legalize otherwise unconstitutional global surveillance cooperation. As so many GIAs seem to be conducting Unlawful Interception, a fatalist and cynic might take the view that that there is no longer any reason to expend effort either negotiating or using MLATs. One might argue if all intelligence is already covertly available to all law enforcement through NSA programs, why bother with MLATs at all? Yet indisputably, MLAT use continues to expand and proliferate.

[160] There are six good reasons why MLAT analysis and analysis of Lawful Intercept in general is legitimate, despite the fact that un-lawful intercept continues apace globally. First, MLATs indicate a need for legal grounds for surveillance by high-MLAT-initiating countries, like

---

[371] *Id.*

[372] Shawn Musgrave, *DEA Teaches Agents to Recreate Evidence Chains to Hide Methods,* MUCKROCK (Feb. 3, 2014), https://www.muckrock.com/news/archives/2014/feb/03/dea-parallel-construction-guides, *archived at* https://perma.cc/92QV-ZUHN.

Canada.[373] Second, they are indicators of prevalence of surveillance targets and collaborators in countries where MLATs cluster, like tiny Cook Islands.[374] Third, not all GIAs from the same country share intelligence data. Thus, LI demonstrably expands surveillance and its measure remains relevant regardless of ULI. Fourth, LI may supplement ULI where GIA's reach is incomplete or unattainable (if such a thing is still possible). Fifth, reliable and significant datasets exist for LI, while few exist for ULI, and the ones that do exist are incomplete and unreliable. So far, no successful attempts to create a trust model based on ULI exist. Sixth, LI country analysis can be viewed as a complement to ULI analysis rather than a substitute.

[161] In terms of the value of MLATs as general surveillance indicators, MLATs can provide legal cover for surveillance by nations that consider themselves law-abiding.[375] While in rogue nations conducting surveillance, the lack of MLATs may not accurately indicate surveillance activity, this does not detract from the fact that MLATs—in combination with other hostility indicators[376]—can provide an overall indication of countries' surveillance traffic and collaboration policies.

[162] Second, analyzing MLATs can shed light on where activity of interest to GIAs may be occurring. For example, the Cook Islands—thousands of miles from anywhere—has approximately 150 treaty relationships.[377] The indicator of activity of interest in this small, ocean-bound nation can indicate something of interest to LI is occurring,

[373] *See In Depth*, *supra* note 62.

[374] *See id.*

[375] *See id.*

[376] *See id.*

[377] COOK ISLAND GOV'T, *Treaty Database: International Treaties*, http://www.mfai.gov.ck/index.php/treaty-database.html, *archived at* http://perma.cc/K8LN-V44Z (last visited Dec. 3, 2015).

whereby it might be logical to conclude the investment of time to establish a legal basis for surveillance has had some justification in the surveillance conducted there.

[163] Third, parallel construction has laid bare that not all GIAs share intelligence. Thus, the NSA's "poor step-siblings" (who must follow the rule of law) demonstrate that for many GIAs, LI—facilitated by tools such as MLATs—clearly expand surveillance, and so still matter.[378]

[164] Fourth, even the most powerful GIA may not have the ability to control online data everywhere in the world, at least not without difficulty. LI provides an additional vector for surveillance beyond where even ULI cannot reach.

[165] Fifth, ULI data (as we have pointed out) is sparse, incomplete, and lacking in credibility. Clearly the optimal surveillance dataset would track all GIAs the world over and score countries by degree of online government surveillance. However, despite diligent effort reviewing existing sources, we (unsurprisingly) remain unaware of a reliable and complete dataset classifying GIA activity for countries around the world. Thus, comparing countries may be impossible on a practical basis, without analyzing what information legally justified LI data can provide.

V. MLATs AND JURISDICTIONAL ARBITRAGE

[166] Having now laid the legal groundwork to understand the motivations and effects of modern MLATs and their role in surveillance, we turn to their application in attacks on online privacy and anonymity tools like Tor. Earlier, we defined MJATs as a class of online multi-jurisdictional, anonymity/privacy tools—including virtual private networks ("VPNs"), proxy servers, and anonymous networks—have

[378] Henrich Glaser-Opitz & Ján Labun, Conference Paper, *Means of Integrating MLAT and ADS-B in up to Date Surveillance Systems*, Int'l Sci. Conference New Trends in Aviation Development 2014, http://www.researchgate.net/publication/271825731, *archived at* http://perma.cc/WV9L-CBAF.

emerged. Examples include JonDos,[379] I2P,[380] Freenet,[381] Lantern,[382] UltraSurf,[383] TorBrowser.[384] For TorBrowser, we noted usage has jumped since 2004 to an average of over 2.5 million daily users worldwide, peaking as high as six million users on high usage days.[385]

[167] MJATs have many uses, and in one way can be thought of as online counter-surveillance tools. The hypothetical American journalist and the Australian whistleblower used Tor to evade government surveillance. Many MJATs use them simply to evade corporate marketing-driven surveillance. In *In Depth: MJAT Jurisdictional Arbitrage Measurement and Technical Experiments*,[386] we review this topic in greater detail, including the mechanics of MJATs, and show how MLATs can be used in their attack. MLATs increase the risk of "breaking" online anonymity tools by allowing countries to collaborate in piecing together encrypted network traffic as it travels through disparate jurisdictions. Anonymity networks such as Tor intentionally route network packets through geographically dispersed checkpoint routers, in order to obfuscate the Internet address and location of the user's device and their destination website.[387] This increases the likelihood that user traffic will

[379] *See JonDo*, *supra* note 22.

[380] *See What Does I2P do for You?*, *supra* note 23.

[381] *See* FREENET PROJECT, *supra* note 24.

[382] *See* LANTERN, *supra* note 25.

[383] *See* ULTRASURF, *supra* note 26.

[384] *See* TOR, *supra* note 1.

[385] *See* TOR METRICS, *supra* note 19.

[386] *See In Depth*, *supra* note 62.

[387] Abdelberi Chaabane et al., *Privacy in Content-Oriented Networking: Threats and Countermeasures*, 43 ACM SIGCOMM COMPUTER COMMC'N REV. 26 (July 2003), at 2–3, http://www.sigcomm.org/sites/default/files/ccr/papers/2013/July/2500098-

travel across multiple legal and other jurisdictions.

A. Legal Threats to Global Online Anonymity Networks: ISPs and IXPs

[168] New adversarial models are necessary to take into account global surveillance and that different governments may pose different, quantifiable risk to anonymous network communications. First, we rank countries by number and nature of intelligence treaties. Second, we bring to light MLAT cartels–groups of cooperating countries. Finally, we demonstrate interlocking cartels can function as super-cartels through legal mechanisms such as JITs. Combined with other measurable hostility factors, we demonstrate a method by which GIA risk per country can be quantified. We show that MLATs are one of several *hostility factors* or *indicators*, which governments can display to anonymous network communications.

[169] Researchers have considered technical attacks against networks, including online anonymity networks. We consider legal attacks against ISPs and IXPs; that is, attacks by governments with legal jurisdiction and control over ISPs and IXPs. In this article, we consider a threat model of local passive adversaries, personified in the form of each of the 191 autonomous governments of the world, based on the ISO 3166 standard. In this model, adversary governments take control in varying degrees of the ability to read online communications traffic flowing over the web as it passes through their own countries, through Internet Service Provider ("ISP") and Internet Exchange Point ("IXP") cables and devices located in their country.

[170] In what jurisdictions do the IXP and ISP lie? In other words, which countries' governments control parts of the path through which your network traffic flows? Do those countries recognize the same standards for privacy as those in the user's home country? Are they more or less

2500102.pdf, *archived at* http://perma.cc/76H2-L67T.

respectful of individual privacy of online communications, including anonymous online communications? What laws exist in those countries, to protect privacy? And, what actual practices exist, regardless of laws?

B. MLAT Attacks: MLATs as an Indicator of Hostility to Privacy

[171] In addition to the matters herein discussed, we build upon the impacts of MLATs in a set of other publications. The use of expanded MLATs has become an indicator of legal hostility to freedom. Countries with a greater number of MLATs indicate their willingness to cooperate in erosion of constitutional freedoms, including intercepting network traffic. In *Jurisdictional Arbitrage,*[388] we identify and define MLAT hostility indicators and other legal hostility factors, and measure the countries of the world by these factors. We explore the implications for anonymous network communications in a series of experiments. We introduce the global MLAT map, the first of its kind. We present our results and conclusions for online privacy tools and attacks through the law. We have identified five hostility factors that indicate a government's legally-encoded hostility to privacy of online communications.[389] Entering into treaties such as MLATs that facilitate cross-border law enforcement and surveillance is one factor identified. In this work, we seek to further the legal groundwork validating this hostility factor as a measure of a country's jurisdictional risk to online privacy. To this end, we have built the first comprehensive repository of MLATs. We have also built the first database of MLAT metadata. We use this database to analyze the growth in MLATs and their global interlocking cartels.

C. Threat, Advisory, and Attack Models

[172] Returning to our initial scenario, we recall the corrupt Australian

[388] *See In Depth*, *supra* note 62.

[389] *See* Sarah Cortes, *Quantifying and Counteracting the Threat of Government Intelligence Agencies Against Tor* (unpublished manuscript) (on file with author).

LEA who wished to track the communications of a journalist who has published leaked whistleblowing documents from a confidential source—revealing the Australian LEA's complicity in illegal narcotics activity. The target journalist lives in New York and is a U.S. citizen. She opens her laptop, goes online and fires up Tor. She communicates with her whistleblowing source in Australia, who faces death if his identity is uncovered—if he is de-anonymized. Her traffic passes through Tor relays in China, Finland, and Malaysia, before proceeding to its final destination, her source's chat server, also in Australia.

[173] We now demonstrate the attack model, the previously discussed MLAT cartel attack. Australia has MLATs with China, Finland, Malaysia, and many other countries. The CSPs and IXPs under their jurisdictions have all long since been required to and have implemented ETSI TS 102 677, facilitating dynamic triggering of surveillance.[390] This process has been administratively and technologically streamlined through the new, "improved" MLAT Central Authority provisions.

[174] As before, the corrupt Australian LEA presses the button, targeting the journalist's network traffic, hoping to find her source. Through traffic correlation and timing attacks, the Australian LEA is able to capture the journalist's outgoing message traffic on its way to the first Tor relay in China. Timing and traffic correlation attacks reveal the destination of the Tor middle relay in Finland, and the LEA captures that traffic as well. A second time, the timing and traffic correlation attacks reveal the destination of the Tor exit relay in Malaysia, and the LEA captures that traffic as well. Finally, a third round of timing and traffic correlation attacks reveal the targeted destination: the journalist's source. The corrupt Australian LEA has just successfully captured the target journalist's network traffic as it passes through Australia, China, Finland, Malaysia and back to Australia.

[175] The content of the journalist's communication is unknown to the corrupt Australian LEA until it leaves the exit relay, as Tor tunnels the

[390] *See ETSI DTS 102 677, supra* note 165.

traffic with encryption. However, once it leaves the exit relay, the LEA can read the now unencrypted traffic, and see the identity of the target whistleblower.

[176] Tor tears down and rebuilds new circuits every few minutes to defeat attacks. Theoretically, a new circuit might be built through a non-cartel partner, cutting off the surveillance. However, the main objective has already been gained once a single circuit de-anonymizes the target. Further, certain high-surveillance countries have expanded MLAT cartels, such that the probability of achieving at least 50% full cartel circuits can be high enough to capture significant information.

[177] This example illustrates the threat model of GIAs collaborating to capture online communications through legal control of IXPs and CSPs outside of their jurisdiction, via MLATs. And, the adversary model, a cartel of collaborating GIAs using MLATs.

[178] In a refinement of the attack model, which we call the MLAT "buddy" attack, the journalist still works at helping her source to blow whistles. However, her Tor traffic path selection algorithm routes her traffic communications through a country that does not collaborate with the Australian LEAs, Iran. Nevertheless, Iran decides to record and store the traffic on its own, as it has a high surveillance hostility factor. At a future date, Iran can decide to supply the "missing link" of recorded traffic and metadata that, together with information recorded by the cartel, can piece together retroactively the whistleblower's identity. Thus, absolute hostility to anonymous network traffic, measured in part by MLATs, is relevant, even without factoring in cartel membership.

[179] In yet another attack model, the same corrupt Australian LEA wishes to surveil traffic form the journalist target to her source whistleblower, the ultimate target. This would be impermissible domestic surveillance, However, by virtue of the traffic being randomly routed outside the U.S. through Tor relays, it may classify it as non-domestic by virtue of its application of Section 215 if FISA. As such, it may apply to its MLAT partners for the traffic.

D. Defenses Against MLAT attacks

[180] In *Quantifying and Counteracting the Threat of Government Intelligence Agencies Against Tor*, we set forth how MJATs, like Tor, can incorporate MLAT metrics into their path selection algorithm. This enables MJATs to avoid countries with high hostility to anonymous network traffic and high collaboration with surveillance cartel partners. Every action to defeat privacy and anonymity, such as expansion of MLATs, produces an equal and opposite reaction, such as improved anonymous networks through path selection modifications to send communications through countries less hostile to anonymous network traffic.

VI. Conclusion, Recommendations, and Future Work

[181] MLATs have significantly expanded in recent years, in number and in scope, with little public attention. We hope future MLAT research will demonstrate that MLATs have indeed expanded the ability of LEAs to solve crime, as the DOJ would assert. We have demonstrated that MLATs have increased the risk of global surveillance, as well as eroded civil liberties to a new, greater degree than has been identified in the past. They have provided at least part of a framework to legalize mass surveillance. They have facilitated imposing technical specifications for surveillance capabilities on CSPs in MLAT cartel jurisdictions. They provide a vector to measure hostility to privacy and anonymous communications by country. Finally, they have facilitated complex technical attacks against online anonymity- and privacy-protecting tools (MJATs), such as Tor, that facilitate surveillance of domestic targets.

[182] We recommend reviewing MLATs comprehensively, rather than on an ad hoc, country-by-country basis, including multilateral MLATs. As the negative impact of MLATs on U.S. citizens and civil liberties becomes clear, policymakers should consider modifications that enable law enforcement to attain international cooperation and assistance, while retaining civil liberties protections. In the meantime, online anonymity-

and privacy-protecting tools can take country hostility factors such as number of MLATs and other factors into account, as well as MLAT cartels, and implement modified path selection algorithms. Thus, the cat-and mouse game will continue.