"WAR CRIMES" AGAINST PRIVACY – THE JURISDICTION OF DATA AND INTERNATIONAL LAW

P. Sean Morris*

Abstract

For Cassius is aweary of the world;
Hated by one he loves; braved by his brother;
Checque'd like a bondman; all his faults observed,
Set in a note-book, learn'd and conn'd by rote,
To cast into my teeth.
— Shakespeare, Julius Caesar, Act IV, Scene iii.

For years, activists have been concerned about assault on one of the most fundamental and cherished freedom that individuals enjoy – the right to privacy. However, in recent years, that right has been gradually loosened due to the widespread use of the Internet. Individuals registering for "free services" such as email provided by Internet communication companies agrees to a number of complex privacy and service agreements. This article sketches an "assault" on data in broad terms and online privacy, and whether governments should access, e.g., personal data, that are located in overseas servers outside the reach of domestic (territorial law) against the backdrop of international law. The article further posits the state of international law and how legislations such as the Stored Communications Act (SCA) in the United States aid and abet "war crimes" on privacy. Of particular interest is also financial data and

 ISSN 1536-7983.

the role of mutual legal assistance treaties (MLATs). The article argues that law enforcement measures which include search warrants for (personal) data such as email contents held on overseas servers poses problems for governments due to jurisdictional issues and the encroachment on the nation state in question sovereignty. Most of the issues raise in this article only scratches the surface of the problem, and therefore, cannot give a full account of all the acts that constitute a "war crime" against privacy.

I. Introduction

Back in 1971, Arthur Miller in his classic text, *The Assault on Privacy*, warned that *cybernetics* instruments of mass surveillance posed "significant threats to personal freedom are presented by the inevitable linking of computers to existing surveillance devices for monitoring people and their communications."[1] Back then, when Miller penned his text, there was no Internet as we know it, and personal computers and networks were novelties, or they were in the process of emerging from the space program and related US Department of Defense programs.[2] There is no doubt that in these modern times, Miller has been vindicated, the moment the Internet became a

*Faculty of Law, University of Helsinki. This is an updated version of a paper written in the summer of 2014. I am grateful to the student editors of this journal for their assistance and efforts to bring this article to publication and for also extending my source citations.

[1] *See* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 43 (Univ. Mich. Press 1971) (explaining how computers will lead to more intrusive surveillance programs).

[2] *See* Brett Frischmann, *Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market*, 2 COLUM. SCI. & TECH. L. REV. 1, 14-18 (2001), (giving an evolution narrative of the internet and efforts of privatization of NSFNET, the precursor of the internet); Barry M. Leiner et al., *Brief History of Internet*, INTERNET SOCIETY (Oct. 15, 2012), *archived at* https://perma.cc/N54R-GXPB (recognizing that prior to 1980, the internet had not been commercialized).

reality, got *commercialized* in the late 1980s and then globalized by the early 1990s.[3]

There are several angles from which Miller's thesis could be developed; however, this article will turn the focus on digital jurisdiction and how laws covering data retention/data grabbing, electronic snooping laws, and even services agreements for commercial free products such as emails, are seen from the perspective of privacy and in the wider context of international law.[4] In this article, most of these laws will be referred to broadly as "information privacy laws." Another key concern discussed in this article is the global storage of private data such as email contents and other online "products" that individuals use, and whether such storage is beyond the reach of national governments.[5]

Harking back to Miller above, we must, turn our attention to some developments in a New York courtroom on April 25, 2014, when a magistrate judge ordered Microsoft Corporation to comply with a search warrant to disclose the private data relating to an email account being held on a server in Ireland.[6] According to the judge, the warrant "is a hybrid: part search warrant and part subpoena."[7] This decision was later upheld by a federal judge on July 31, 2014.[8]

---

[3] *See* e.g., Frischmann, *supra* note 2, at 16 (discussing the role of the NSFNET in the commercialization of the internet); *see also* Leiner, *supra* note 2 (outlining the historical events leading to the commercialization and globalization of the internet).

[4] See *infra* Section II (analyzing data privacy laws from an international perspective).

[5] *See* Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, HOGAN LOVELLS WHITE PAPER 1 (May 23, 2012), *archived at* https://perma.cc/Z23M-AD2L (discussing the government's access to Cloud data in different jurisdictions).

[6] *See* In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467, 477 (S.D.N.Y. 2014) [hereinafter Microsoft Search Warrant] (indicating the Court's interpretation of legislation concerning extraterritorial application warrants).

[7] *See id.* at 471 (describing an unconventional order combining the initial procedure to obtain a warrant resulting in an execution of a subpoena).

[8] *See* In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., Nos. M9-150, 13-MJ-2814, 2014 WL 4629624, *1 (S.D.N.Y. Aug. 29, 2014) (affirming rulings from original case)*; see also* Microsoft Corp. v. United States, 829 F.3d 197, 200 (2d Cir. 2016) (explaining how the original case made its way to the Second Circuit and became known as "Microsoft-Ireland"). In this ruling, the court sided with Microsoft and argued that the SCA was not designed to apply extraterritorially. *Id.* at 211. Since this article was written,

This example involving Microsoft and the U.S. government's attempt to obtain private data for one of Microsoft's user, whose data is located outside of the U.S. in Ireland develops some of the broader problems that faces international law.[9]

There are two key aspects of the case (a) whether Microsoft should comply with the search warrant to hand over data located overseas, and (b) whether U.S. laws should be given extraterritorial effect.[10] These two aspects raise questions regarding the reach of domestic laws and their effect on privacy and private data.[11] Most of the domestic laws concerned either give law enforcement agencies the power to retain or syphon (duplicate) individual online activities

based on the original ruling in 2014, a number of commentaries appeared in various journals looking at one of the main implications: the extraterritoriality of U.S. laws, which is also discussed in this paper. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 326, 383 (2015) (opposing extraterritorial law enforcement that is encouraged by modern electronic data storage); Russell Hsiao, *Implications for the Future of Global Data Security and Privacy: The Territorial Application of the Stored Communications Act and the Microsoft Case*, 24 CATH. U. J. L. & TECH. 215, 217 (2015) (looking at one of the main implications of the extraterritoriality of U.S. laws); Lindsay La Marca, *I Got 99 Problems and a Warrant is One: How Current Interpretations of the Stored Communications Act Offend International Comity*, 44 HOFSTRA. L. REV. 971, 972 (2016) (describing Microsoft's current practices as overreaching with the Fourth Amendment). Some articles also looked at the July 2016 ruling and discuss in general other aspects of international law and privacy. *See, e.g.*, Ned Schultheis, *Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the U.S. Cloud Storage Industry*, 9 BROOK. J. CORP. FIN. & COM. L. 661, 661 (2015) (looking at the July 2014 ruling and discussing in general other aspects of international law and privacy); Ilina Georgieva, *The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR*, 31 UTRECHT J. OF INT'L AND EUR. L. 104, 104 (2015) (characterizing privacy as a key component in international law); Cedric Ryngaert, Editorial, *Symposium on Extraterritoriality in EU Data Protection Law*, 5 INT'L DATA PRIVACY L. 221, 221-22 (Oct. 7, 2015) (explaining that international jurisdiction is only limited by extreme circumstances); Bo Zhao, *The Internationalisation of Information Privacy: Towards a Common Protection*, 2 GRONINGEN J. INT'L L. 1, 1 (2014) (highlighting the broader commentary on privacy and international law in general).

[9] *See Microsoft Corp.*, 829 F.3d at 200-01 (showing Microsoft's unwillingness to comply with a federal warrant and the government's ability to induce compliance).

[10] *See id.* at 201 (identifying the warrant dispute as the main issue of the case).

[11] *See id.* (noting that Congress intended warrant provisions to reach outside of the U.S.).

or access general data storage facilities such as those in financial transactions.[12] The question is how much legality exists in these practices within the context of international law.[13] In terms of the latter, consider financial databases such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system[14] as examples of data that can be (*un*)lawfully accessed, and that any such access, is part of systematic effort to exert control over all forms of data that traverses the Internet.[15] The claim of "war crimes" against privacy in this article refers to those acts undertaken by governments to access private data of individuals in order to make allegations of criminal enterprising activities, and also the access to data by illegal methods.[16]

The term "data" is use broadly in this article, and sometimes refers to "personal data" including data of private individuals held on email servers; "corporate data;" and "non-corporate data," such as SWIFT, among others.[17] As such, this article focuses on how governments intercept private data and asks whether national *information privacy laws* should be applied extraterritorially in the absence of a global and standardized regime of international information privacy

[12] *See id.* at 227 (illustrating that domestic laws allow law enforcement to obtain information from a service provider). 18 U.S.C. § 2703(b)(1)(A) summarizes specifically "the procedural mechanism to allow the government to 'require a [service provider] to disclose the contents of [certain] electronic communication[s]' *without notice to the subscriber or customer*.'" *Id*. (emphasis in original).

[13] *See id.* (showing that warrants to obtain emails and other information are not traditional search warrants and therefore, might not authorize companies to release the data of clients without their consent): *see also*, Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985 (1983 (discussing a range of issues, some of which are also raised in this article).

[14] *See* Gloria González Fuster et al., *SWIFT and the Vulnerability of Transatlantic Data Transfers*, 22 INT'L REV. L. COMPUT. & TECH. 191, 192 (2008) (identifying SWIFT as an example of financial databases).

[15] *See id.* (noting that there is a fundamental problem with the regulation of international data transfers).

[16] *See id.* at 194-95 (disagreeing with SWIFT's perspective that its activities in transferring personal data were illegal).

[17] *See id.* at 191 (clarifying that data refers to both personal data and corporate data).

laws.[18] From this point of view, the article raises questions on the international nature of information privacy laws and suggests that questions pertaining to private data, under the circumstances discussed in the article, are no longer for national states, but are also a concern for international law and that bodies, such as the International Law Commission ("ILC"), should look into the relationship with data grabbing laws that are enacted quickly around the world.[19]

Because this article addresses the body of law, referred to in this article as *informational privacy laws* concerning data in broad terms, there is the need to be clear on terminologies. Both the term "data protection" and "privacy" are sometimes used interchangeably, or on other occasions, with specific reference, depending on the context.[20] Also, the terms refer to the system of laws known as informational privacy laws building on the legal differences used in common law and civil law.[21] Thus, what some continental Europeans call "data protection", others may simply refer to as "privacy."[22] This explanation is for the purposes of this article, because strictly speaking both bodies of laws – data protection laws and privacy laws – are completely different when one takes into account the narrow focus of "privacy" as opposed to the broader "data protection" terminology.[23]

---

[18] *See id.* (noting that U.S. authorities may secretly access information on financial transactions taking place in the European Union and this may raise issues regarding the protection of data guaranteed to European citizens).

[19] *See id.* (identifying that different European data protection authorities are attempting to mitigate illegal data mining through independent legislation governing their regions).

[20] *See* Francoise Gilbert, *Privacy v. Data Protection. What is the Difference?*, FRANCOISE GILBERT (Oct. 1, 2014), *archived at* https://perma.cc/BC5D-R8JP (stating how "privacy" and "data protection" can be used differently, depending on the country).

[21] *See* Samuel Wee Choong Sian, *Privacy Law: A Case for the Protection of Informational Privacy in Singapore*, 31 SING. L. REV. 143, 162 (2013) (explaining the differences in privacy law when the United Kingdom was a civil law and a common law country).

[22] *See* Gilbert, *supra* note 20 (drawing distinctions between the use of "privacy" and "data protection" on different continents).

[23] *See* Juliane Kokott & Christoph Sobotta, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INT'L DATA PRIVACY L. 222, 225 (2013) (discussing the differences between privacy and data protection in the jurisprudence of Europe's two highest courts).

The gist of this article is a discussion on both bodies of law that protects privacy and private/personal data, and in this regard, both bodies of law shall be construed under the roof of information privacy laws.[24] There is third body of law, which forms part of the broader theme of this article, namely, data retention laws or data grabbing laws (snooping legislation) that require the storage of data; it is this body of law that this article explores arguments on as enablers of "war crimes" against privacy.[25]

The concept of "personal data" is standardized in numerous legal instruments, for example, in regional,[26] domestic and semi-international (soft) law instruments such as the Organization for Economic Cooperation and Development ("OECD") Data Guidelines.[27] Moreover, it is such description that is found in the number of cases

[24] *See id*. at 222 (introducing the scope of European court's jurisdiction).

[25] *See Investigatory Powers Act 2016: Chapter 25*, LEGISLATION.GOV.UK 9 (2016), *archived at* https://perma.cc/N79T-ZWHD (giving an example of how the UK is one of a number of countries that have passed legislations giving law enforcement authorities unprecedented powers to access the private and personal data of individuals online, and also requiring internet communication companies to store data on servers in their respective jurisdiction). The UK's Investigatory Powers Act, which had been on the drawing board since 2014, was passed in the Houses of Parliament in November 2016. *Id.* at 1. The Investigatory Powers Act enabled authorities to intercept and store all forms of data from the internet. *Id.* at 9. *See also* Emma Woollacott, *UK Joins Russia And China In Legalizing Bulk Surveillance*, FORBES, *archived at* https://perma.cc/4Q3D-SFSE (indicating that *Russia* also passed similar laws in 2016).; Evgenlya Melnlkova, *Yarovaya Law. The Death Of The Russian Constitution.*, WORLD POST (July 22, 2016), *archived at* https://perma.cc/8PU4-GFUE (noting that the Russian surveillance law is often referred to as "Yarovaya Law," after its author).

[26] *See* Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) 31, 38 (defining personal data and discussing the free movement of such data).

[27] *See* Org. for Econ. Cooperation and Dev., *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, art. 1(b), 2013 O.J. (C 80) 11 [hereinafter *OECD Guidelines*] (citing broadly to an example of a legal instrument that standardizes personal data).

that are litigated, in particular Europe, or other cases that are the target of litigation.[28] Thus, for example in cases such as *Bonnier v. Perfect Communication*[29] at the Court of Justice of the European Union ("CJEU"), that Court, echoing the legislation, reaffirmed that personal data is "any information relating to an identified or identifiable natural person."[30] Similarly, at the European Court for Human Rights ("ECtHR"), in *Copland v. the United Kingdom*,[31] the notion of personal data was similar confirmed, in particular as it is defined under Article 8 of the European Convention on Human Rights ("ECHR").[32] The *Copland* decision is interesting as it relates to information derived from the monitoring of personal Internet usage.[33] The monitoring of personal Internet usage and the data such usage contains, such as that of personal email, was the subject of the *Microsoft Search Warrant* case.[34]

In this article, "private data" is used to refer to arguments relating to the case, as oppose to "personal data". The broad point raised by that case, the extraterritoriality of U.S. laws, is of serious

[28] *See* Laraine Laudati, *Summaries of EU Court Decisions Relating to Data Protection 2000-2015*, OLAF (Jan. 28, 2016), *archived at* https://perma.cc/UJB2-7LRZ (identifying several cases litigated in the European Union).
[29] *See* Case C-461/10, Bonnier Audio AB v. Perfect Communication Sweden AB, [2012] 2 C.M.L.R. 42 (discussing broadly on the protection of personal data in various domains).
[30] *See id.* at ¶ 5 (discussing prior court rulings on legislation regarding personal data and indicating how the present case is different).
[31] *See* Copland v. United Kingdom, [2007] E.C.H.R. 253, ¶ 44 (considering that the storage of personal information without knowledge of the storage being used is a violation of one's right to privacy).
[32] *See* Data Protection Act 1988 (Act No. 25/1988) (Section 1) (explaining that "personal data" means data relating to a living individual who is or can be identified from data or from data in conjunction with other information that is in, or is likely to come into, the possession of a data controller")*; see also European Convention on Human Rights*, EUROPEAN COURT OF HUMAN RIGHTS, *archived at* https://perma.cc/N56D-HG8K, at 10 (explaining that everyone has the right to privacy).
[33] *See Copland*, [2007] E.C.H.R. 253 at ¶ 41 (describing the court's reasoning on how personal information relates to Internet usage).
[34] *See Microsoft Corp*., 829 F.3d at 219 (exemplifying a case on email search warrants).

concern in relation to international law and the jurisdiction of digital data stored on servers overseas.[35]

II. The Nature of Data Under International Law and an Example of Data That is the *Target* for "War Crimes"

Ever since the Internet allowed the cross-border flow of information more rapidly, regulators and policy makers have been struggling with questions of privacy.[36] Moreover, the cross-border flow of data poses severe problems for international law because data located overseas are not subjected to extraterritorial application of domestic law, for the reason that such act would be generally a gross violation of a country's sovereignty.[37] However, on the other hand, because of the number of actors involved in trans-border data, who are subjected to both domestic law and international law, questions pertaining to jurisdiction poses greater challenges to international law.[38] So, what then, to do under these circumstances? First, one would actually need to understand (a) what kind of data is vulnerable to cross-border transfer, and (b) the state of international law, and how all of this is linked to domestic laws on data grabbing (acquisition and retention). The rest of this article will subsequently address these issues and also how countries are creating a new international legalism with data protection laws in relations to privacy.

Prior to the Internet the trans-border flow of data was minimal and limited to methods such as fax machines, telephones, letters and telegrams, whilst financial transactions such as wire transfers prior to the Internet were also a source of the trans-border flow of data.[39] Today, while these conduits for data transmissions are still around, they

---

[35] *See id.* at 220 (discussing the international implications of a warrant even though it was only intended to apply in the U.S.).
[36] *See* Maxwell & Wolf, *supra* note 5, at 2 (explaining European fear of U.S. cross-border access of data).
[37] *See* Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 47-49 (2001) (describing how a sovereign's cross-border conduct against another individual may cause an international law violation).
[38] *See id.* at 39 (explaining the challenges that states face enforcing domestic laws extraterritorially).
[39] *See* Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L. J. 393, 394 (2013) (discussing Article 19 of the ICCPR as it relates to new technol-

are largely replaced by the Internet which facilitates the faster transmission of data across borders.[40] Furthermore, because *zeegatons* of pages of data are created everyday with the availability of more data creation devices, such as modern smart phones, tablets, laptops, personal computer among others, such data becomes the target of criminals, law enforcement authorities, commercial entities and "hackers."[41] The protection of such data varies by countries, with some regions such as the *supra-federal* European Union having strong privacy protection laws, while other countries such as the U.S. and some in Africa or South America have either different standards for the protection of privacy or mediocre and weak privacy protection laws.[42]

Internet created data (e.g., contents) by private individuals that is stored on commercial servers is a commodity in the eyes of the commercial operators and the personal property of the individual.[43] For commercial entities which store an individual's private data (contents), that data is also the "property" of those commercial entities, or the data creator has given his or her explicit consent to the commercial operating entities to use such data for their own commercial gains.[44] Another explicit consent that private individuals give is for

ogies)*; see also* Craig T. Beling, Note, *Transborder Data Flows: International Privacy Protection and the Free Flow of Information*, 6 B.C. INT'L & COMP. L. 591, 591 (1983) (explaining how transborder data flows manifested themselves in 1983).

[40] *See* Leiner et al., *supra* note 2 (highlighting the global reach of the internet in contemporary society).

[41] *See Cyber Security Planning Guide*, FEDERAL COMMUNICATIONS COMMISSION MD-1 (2012), *archived at* https://perma.cc/W6LV-GQCW (describing cyber security threats to mobile devices brought into the workplace).

[42] *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1318 (2000) (explaining how privacy rights for data vary across the world).

[43] *See* Corien Prins, *When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?*, 3:4 SCRIPTED 270, 271 (June 2006) (comparing the commercial and private nature of personal data).

[44] *See Microsoft Services Agreement*, MICROSOFT (July 15, 2016) [hereinafter *Microsoft MSA*], *archived at* https://perma.cc/B6DH-3APD (granting Microsoft the worldwide right, without charge, to use Content as necessary).

law enforcement agencies to access their data that commercial entities, such as Apple, hold on them.[45] These consents are normally given at the click of a button when the potential private individual accepts the terms and conditions and privacy policies of the commercial data hosting operators.[46]

Under international law, the access of data becomes an issue when it involves law enforcement irrespective of the location of the data, because it raises a number of questions on sovereignty, jurisdiction, ownership, obligations of commercial hosting entities and the initial consent by the individual when accepting the terms and privacy policies of the commercial hosting entity.[47] Under the Universal Declaration of Human Rights ("UNDHR")[48] and the International

---

[45] *See Privacy Policy*, APPLE (Sept. 12, 2016), *archived at* https://perma.cc/5C2L-FMRH (setting out the terms of Apple's privacy policy). Apple states that disclosure to third parties including law enforcement agencies may sometimes be necessary:

> It may be necessary – by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence – for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.

Id.

[46] *See id.* (explaining that the privacy policy is adopted at the time the product is activated and the activator consents to the privacy terms while activating the phone).

[47] *See* Kate Westmoreland, *The Global Corporate Citizen: Responding to International Law Enforcement Requests for Online User Data*, HARVARD JOURNAL OF LAW & TECHNOLOGY (Aug. 13, 2015), *archived at* https://perma.cc/MD44-SKRV (summarizing that privacy issues become more complex when they involve users and governments from many different countries).

[48] *See* G.A. Res. 217 A (III), art. 12, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter UNDHR]. Article 12 of the UNDHR reads, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.*

Covenant on Civil and Political Rights ("ICCPR")[49] there are identical provisions for the right to privacy.[50] Together these two instruments plays a vital role in how data protection is covered in an international legal context and also serves as further attempts for global privacy laws.[51] Developments in Europe, and in particular, the ECtHR gave data protection a global appeal, and from there, data protection spread it wings – soaring through "civilized" and like-minded nations to include similar conventions in South America.[52] The recently revised OECD Guidelines on the trans-border flow of data and the United Nations ("UN") data files guidelines[53] also play key roles in the international legal sphere of data protection.[54]

One of the areas in which the question of data has been most attractive for governments and criminals is that of financial data and its storage.[55] The use of financial sanctions by (western) governments has always been the most effective tool in putting a squeeze on their targets, whether it be a nation state, a non-state entity such as

---

[49] *See* G.A. Res. 14668, art. 17, International Covenant on Civil and Political Rights (Dec. 19, 1966) [hereinafter ICCPR]. Article 17 reads: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attack on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

[50] *See* ICCPR, *supra* note 49 (inferring that these two international documents are the same in regard to the right of privacy).

[51] *See* ICCPR, *supra* note 49 (stating that these two international documents are key documents in enforcing international privacy laws).

[52] *See* American Convention on Human Rights, 1144 U.N.T.S. 17955, at 144 (recognizing individuals' protected rights in foreign countries and extending those protections to countries affiliated with this treaty to be enforced on July 18, 1978).

[53] *See* G.A. Res. 45/95, Guidelines for the Regulation of Computerized Personal Data Files (Dec. 14, 1990) (documenting "procedures for implementing regulations concerning computerized personal data files").

[54] *See OECD Guidelines*, *supra* note 27 (referencing existing guidelines on transborder data flow).

[55] *See* Daniel Gutierrez, *Big Data for Finance – Security and Regulatory Compliance Considerations*, INSIDEBIGDATA (Oct. 20, 2014), *archived at* https://perma.cc/XW7Q-AMD9 (discussing financial institutions are high priority to protect against cybercrime).

Al-Qaeda, or those in the inner circle of a president with which Western states must deal.[56] Financial sanctions are easy because financial transactions and individual relationship with banks contain a wealth of data that can trace every penny an individual spends.[57] Furthermore, data at financial institutions have been building up ever since wire (electronic) transfer was made possible and as well as the emergence of credit cards.[58] American financial processing institutions have always had a grip on the latter through MasterCard Inc., Visa Inc., and American Express Inc., and in recent years, American government departments such as the Treasury have also been able to access non-American financial databases involved in financial transactions.[59]

For individuals to form a relationship with a financial transaction firm, in most cases they often need acceptable government identification to start that relationship.[60] Most financial institutions in countries such as the U.S., the U.K., Europe, and practically all over the world, are also required to report to a government oversight agency as part of counter terrorism efforts, large financial transactions.[61] In this reporting process the massive amount of data that is

---

[56] *See* Marcus Boomen, *The Effectiveness and Ethics of Economics Sanctions*, SEVEN PILLARS INSTITUTE (July 16, 2014), *archived at* https://perma.cc/7L2H-S42N (weighing the effectiveness and ethics of economic sanctions).

[57] *See* Barry E. Carter & Ryan Farha, *Overview and Operation of U.S. Financial Sanctions, Including the Example of Iran*, 44 GEO. J. INT'L L. 903, 904 (2013) (stating how financial sanctions focus on funds to and from the target country, individual, or other entity).

[58] *See id.* at 905-06 (discussing wire transfers and how banks affect those transfers).

[59] *See* James Peter Rubin, *Visa, AmEx, MasterCard, Discover—What's the Difference?*, CREDITCARDS.COM (Apr. 9, 2009), *archived at* https://perma.cc/9QGW-CBDV (distinguishing the world's most popular credit card companies)*; see also Office of Foreign Assets Control*, U.S. DEPARTMENT OF THE TREASURY, *archived at* https://perma.cc/LQ5Q-JT9N (describing the U.S. Treasury's interactions with foreign financial institutions).

[60] *See Customer Identification Programs for Financial Transactions*, PRIVACY RIGHTS CLEARINGHOUSE (Sept. 21, 2016), *archived at* https://perma.cc/3P4M-VS52 (indicating that government identification is necessary for forming a relationship with a financial institution).

[61] *See Combating Transnational Organized Crime*, FINANCIAL CRIMES ENFORCEMENT NETWORK, *archived at* https://perma.cc/5RFU-FBJR (depicting how the Financial Crimes Enforcement Network combats transnational organized crime).

passed on to governments makes it easy for governments to build a financial data profile on individuals.[62] Moreover, governments can subpoena financial transactions[63] that cross borders because of the standardized SWIFT system.[64] The SWIFT system is itself a problem under international law because although a private non-profit making entity, its global reach and influence in international financial transactions makes its database and wide reach, the target of law enforcement agencies.[65] Although not a bank, for all intents and purposes, the SWIFT system is the "nerve center of the global banking industry."[66]

The operators of the SWIFT system have been taken to courts in the U.S. for unlawfully disclosing private data (e.g., financial records)[67] and this goes to show the extent the problem of disclosing data located in other jurisdictions poses for international law.[68] Once governments have access to these financial data profiles and transactions, it equips the government to carry out at will "war crimes" against privacy.[69] Take for example the instance when a Danish man paid for Cuban cigars and his payment was intercepted by American

---

[62] *See id.* (detailing the way governments interact and exchange financial data).
[63] *See* Walker v. S.W.I.F.T. SCRL, 517 F. Supp. 2d 801, 804 (E.D. Va. 2007) (noting how the Treasury Department issued administrative subpoenas regarding financial transmissions).
[64] *See* Susan V. Scott & Markos Zachariadis, *A Historical Analysis of Core Financial Services Infrastructure: Society for Worldwide Interbank Financial Telecommunication (SWIFT)* 11 (London Sch. of Econ. Info. Sys. & Innovation Grp., Working Paper Ser. No. 182, 2010) (discussing the standardization of the SWIFT system).
[65] *See id.* at 19 (articulating the issues the SWIFT system raises in the international community).
[66] *See* Amidax Trading Group v. S.W.I.F.T. SCRL, 671 F.3d 140, 143 (2d Cir. 2011) (highlighting the important role SWIFT plays in the global financial industry).
[67] *See Walker*, 517 F. Supp. 2d at 804 (explaining the allegations against SWIFT operators for disclosing confidential information).
[68] *See id.* at 804 (opining on international law issues in financial transactions).
[69] *See* Jeffrey B. Ritter, *Current Issues in Electronic Data Interchange: Defining International Electronic Commerce*, 13 NW. J. INT'L L. & BUS. 3, 21 (1992) (predicting governmental abuse when given access to electronic financial data).

operatives,[70] or similarly, when the SWIFT was on the dock for allegedly disclosing Canadian financial transactions illegally.[71]

The SWIFT system started out as a tightly knit group and registered under Belgian Law in 1973 with the purpose of providing secure transfer of intercontinental financial transactions.[72] Its aura and might grew and it became a colossal repository[73] for financial data and it is now a powerful entity so much so that it "routes more than 11 million financial transactions each day."[74] As an international cooperative consortium that spans over two hundred countries and servicing almost eight thousands banks,[75] the amount of data SWIFT amassed since its founding, and more so, since faster electronic method such as the Internet allowed it to gather and store more data – SWIFT has become more than a nerve center for the global financial industry; it is also the very *oxygen* that drives global commerce and shapes every action in a society that relies on financial transactions.[76] But such oxygen can be diluted by the very process that generates it and when such dilution occurs the true problems in the system can reveal themselves.

Unlawful access to the SWIFT system by governments is only one example of potential "war crimes" against privacy, but more so,

---

[70] *See Danish policeman caught in American terrorist networks*, BERLINGSKE (Feb. 26, 2012), *archived at* https://perma.cc/9YBV-6Q3R (explaining that the United States government has the authority to police foreign financial transactions).
[71] *See The Personal Information Protection and Electronic Documents Act (PIPEDA)*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (Sept. 9, 2016), *archived at* https://perma.cc/2Q8S-MFNB (outlining findings under this act)*; see also* Jennifer Stoddart, *Privacy Commissioner of Canada v. SWIFT: Report of Findings*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (Apr. 2, 2007), *archived at* https://perma.cc/765X-Z7U3 (describing the circumstances that lead to the Canadian government's investigation).
[72] *See id.* (articulating SWIFT's background in providing secure financial transactions).
[73] *See* Walker v. S.W.I.F.T. SCRL, 491 F. Supp. 2d 781, 785-86 (N.D. Ill. 2007) (illustrating SWIFT's dominance in the financial industry).
[74] *See id.* at 786 (detailing the amount of financial transactions SWIFT routes on a daily basis).
[75] *See id.* (highlighting the number of countries and financial institutions SWIFT services).
[76] *See Introduction to SWIFT*, SWIFT (2016), *archived at* https://perma.cc/U7U6-P74U (showing how SWIFT reaches over 11,000 banks and securities organizations).

access to the SWIFT system reveals the sad state of international law.[77] How is it that a NGO consortium that controls the world's financial *oxygen* of commerce with personal/private data can be turned over to a (single) state does not draw the wrath and ire of international law practitioners or the system of international law itself?[78] This is because of the troubled state of international law in terms of access to data and data retention, and more so because there is no international legal instrument that can regulate access to personal/private data, in particular when that data is the subject of trans-border transmission.[79] In this regard, given the lack of principles of international information privacy laws to apply to data transmission when disputes that involve states occur, then at least one of the state parties to the dispute will attempt to apply its domestic laws extraterritorially.[80] Such steps are taken even when the other party to the state has data protection laws both at the national level or *supra-federal* level.[81]

But discussing the SWIFT system as one example of where "war crimes" against privacy can be potentially committed only reveals more problems that are inherent in the system that involves private data protection.[82] A more concrete example is discussed in the next section, which juxtaposes personal/private data over the Internet and the commercial operators that maintain that personal/private data with how international law interacts with domestic law.[83] But there is another point which must be made before turning to that argument,

---

[77] *See Amidax Trading Group*, 671 F.3d at 143 (expressing the extent of privacy safeguards).
[78] *See id.* (questioning SWIFT's judgment in providing the government full data access).
[79] *See* Steven Bellman et al., *International Differences in Information Privacy Concern: Implications for the Globalization of Electronic Commerce*, *in* 31 ADVANCES IN CONSUMER RESEARCH 362 (2004) (explaining that countries differ on views of privacy and security issues).
[80] *See* Beling, *supra* note 39, at 593 (discussing different approaches to international data protection).
[81] *See* Beling, *supra* note 39, at 593 (exemplifying two international agreements on data protection).
[82] *See Amidax Trading Group*, 671 F.3d at 143 (explaining prompted negotiations concerning scope of disclosure of SWIFT data).
[83] *See infra* Part III.

which is the new international legalism through data protection laws.[84]

Since March 2015 the number of countries with data protection and privacy laws continues to grow,[85] while other international actors such as international organizations and NGOs also have guidelines pertaining to information privacy laws.[86] But the plethora of data protection laws adopted since the UNDHR and the ICCPR not only represents a new era of international legalism, but it is also encouraging other states that were normally skeptical of data protection and privacy rules to create back door legal channels to conform to this new international legalism in information privacy law.[87] However, the more troubling thing about this new form of international legalism is that what was initially "the protection of data" and or "privacy" is now about the complete opposite, with a new layer for the erosion and grabbing of personal/private data from the individual slowly taking shape through data retention laws, or laws that were once dormant.[88]

These two seemingly opposite objectives of the new international legalism in information privacy laws creates paradoxical situations for the erosion of those same rights by internet monitoring laws that are meant to "grab" data from the individual in the name of "security" and or the enforcement of laws pertaining to a number of areas such as terrorism, surveillance among others.[89] Moreover, the legal pathway to data grabbing is typically seen in countries with

---

[84] *See* Theodore J. Kobus et al., *2015 International Compendium of Data Privacy Laws*, BAKERHOSTETLER, iv (2015) (providing overview of data protection laws globally).

[85] *See id.* (pointing out the increasing number of countries with policies directed at addressing privacy concerns arising from data protection issues).

[86] *See OECD Guidelines*, *supra* note 27, at 11-12 (elaborating on guidelines pertaining to international organizations and NGOs).

[87] *See* L. Richard Fischer, *Privacy and Accuracy of Personal Information*, 3 N.C. BANKING INST. 11, 16-21 (1999) (summarizing the influence of international privacy developments).

[88] *See* Joseph Menn & Dustin Volz, *Apple Case Exposes Ongoing Government Rift Over Encryption Policy*, 30 No. 7 WESTLAW J. WHITE-COLLAR CRIME 6, *1 (2016) (acknowledging unintended interpretation of privacy law could lead to lawsuits similar to *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant*).

[89] *See* Ian Brown & Douwe Korff, *Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online*, GLOBAL NETWORK INITIATIVE (June 14,

Common law legal systems where they are able to enact new provisions that allow for data grabbing, and this has been manifested in legislation such as the Investigatory Powers Act 2016 in the U.K. and similar laws in countries that are part of the Anglo-Alliance Five Eyes Nations[90] which is comprised of the U.K., U.S., Canada, Australia and New Zealand.[91] This alliance and its approach to data grabbing is also creating a different paradigm in international legalism of information privacy laws, creating a disguised empire of information in the process.[92] This disguised empire is part of a globalization trend where *dominions* of legal regulations are created, such as in security law, and the individual is *subject* of the dominion without the right to personhood.[93]

2012), *archived at* https://perma.cc/E23U-2KRF (explaining that effective counter-terrorism and protection of human rights are complementary); *see also Investigatory Powers Act 2016: Chapter 25*, *supra* note 25, at 277 (explaining the balance between the Investigatory Powers Act 2016 and the Counter-Terrorism Act 2008).

[90] *See e.g.*, Ian Brown, *Witness Statement*, PRIVACY NOT PRISM 14 (Sept. 27, 2013), *archived at* https://perma.cc/U6B8-G8LF (discussing the Five Eyes Nations).

[91] *See The Five Eyes*, PRIVACY INTERNATIONAL, *archived at* https://perma.cc/KY6X-KX5V (giving background information as to the members of the Five Eyes Nations, and the reason behind the group's creation).

[92] *See* Monika Zalnieriute, *An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance*, 23 INT'L. J. L. INFO. TECH. 99, 120 (2015) (highlighting the issues concerning a collection and sharing of data that created a "parallel universe"); David G. Barnum, *Warrantless Electronic Surveillance in National Security Cases: Lessons from America*, 5 EUR. HUM. RTS. L. REV. 514, 517-22 (2006) (discussing constitutional issues in electronic surveillance); *IPT/15/110*, THE INVESTIGATORY POWERS TRIBUNAL 3 (Oct. 17, 2016), *archived at* https://perma.cc/XR8P-6HR8 (handing down the judgment in a tribunal case, which raised issues of privacy, data protection, data retention, surveillance, and abuse of data gathering, among others).

[93] *See id.* at 101-02 (discussing a loss of privacy occurs when all details of personal life can be analyzed through metadata).

III. Search Warrant and Overseas Data: Problems in International Law

One obstacle that countries will need to overcome is how to legally access data that are stored in other jurisdictions.[94] Can country X (which is not a part of a group of states that forms a single market and political entity) gain access to Citizen Eurosky's data in Country Y if that country has laws that restrict or prohibit access to and/or the transfer of such data outside its borders?[95] Or could a reasonable case be made for the access to such data under mutual legal assistance treaties ("MLATs")?[96] If not, could Country X apply its own data laws extraterritorially to gain access to the personal data of Citizen Eurosky?[97] In short the answer is "no," and even under international law it is also a "no-no," despite what a lower court in New York thought in 2014.[98] However, the lower court's decision was overturned in 2016.[99]

An internal search warrant issued for the digital contents of an individual is probably a formality and offers some form of transparency, if one should take into account the nature and power of agencies such as the National Security Agency ("NSA") in the U.S. or the U.K.'s Government Communications Headquarters ("GCHQ") to intercept data and in particular, data communicated over the internet.[100]

Commercial entities that store private data, such as Apple, Inc., generally inform those individuals that their data can be accessed by governments when necessary.[101] It was a similar point the

---

[94] *See* Bellia, *supra* note 37, at 39 (describing the difficulty experienced by nations while conducting cross-border investigations).
[95] *See, e.g.*, Bellia, *supra* note 37, at 61-64 (discussing the legal nuances of cross-border searches under international law).
[96] *See, e.g.*, Bellia, supra note 37, at 50-54 (exploring mutual legal assistance treaties in both theoretical and practical terms).
[97] *See, e.g.*, Bellia, supra note 37, at 63-65 (providing a general discussion of issues arising with extraterritorial conduct).
[98] *See Microsoft Corp.*, 829 F.3d at 200-01 (summarizing Microsoft's argument regarding overseas data and the district court's unfavorable decision).
[99] *See id.* at 201-02 (reversing the lower court's decision).
[100] *See* Georgieva, *supra* note 8, at 104-05 (discussing government surveillance power to conduct its expansive activities secretively).
[101] *See Privacy Policy*, *supra* note 45 (disclosing Apple's policy regarding governmental access to stored data).

government was keen on reinforcing in its submission to the federal judge in the *Microsoft Search Warrant* 2014 decision and to that effect, in its opening salvo, the government noted:

> [A]ll Microsoft account data, whether stored in the United States, the Dublin data center, or in any of Microsoft's many other locations throughout the world, are under the control of and readily available to Microsoft's employees in the United States, who can access the data using a program designed for that very purpose.[102]

Interestingly, in the Google "right to be forgotten" case in Europe,[103] a similar position was taken by Google when it claimed that the processing of personal data was carried out by Google, Inc. without the intervention of its Spanish subsidiary, since the subsidiary was merely for advertising purposes only,[104] which was a claim the court dismissed.[105]

But it is unlikely that companies such as Microsoft, Google, Twitter, Apple, and Facebook among others can *unlawfully* disclose personal data of their users. In fact, these companies explicitly state that that they cooperate with law enforcement agencies and follow applicable law to disclose personal data. For example, Microsoft has explained to users, via its service agreement why it shares a user's personal data.[106]

---

[102] Brief of Government in Support of Magistrate's Decision at 3, Microsoft Search Warrant, No. 13-2814 (S.D.N.Y. July 9, 2014), ECF No. 60.

[103] *See* Case C-131/12, Google Spain v. Agencia Española de Protección de Datos, 2014 E.C.R. I-0000 ("regarding the scope of the right of erasure and/or the right to object, in relation to the 'right to be forgotten'").

[104] *See id.* at ¶ 62 (stating that processing of personal data is carried out exclusively by Google Inc., and not Google Spain).

[105] *See id.* at ¶ 138 (noting that data processing is carried out in Spanish territory and cannot violate Directive 95/46).

[106] *See Microsoft MSA*, *supra* note 44, at 4 (stating that the Agreement incorporates the Privacy Statements by reference). "By using the Services or agree to these terms, you consent to Microsoft's collection, use and disclosure of your Content and information as described in the Privacy Statements." *Id.*

> . . . [W]e will access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to:
> 1. Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies . . . .[107]

The above quotation is generally across the board for Microsoft services and the main thing is that it highlights Microsoft's cooperation with law enforcement authorities.[108] But the quotation is crucial because, first and foremost, the average user of internet services, rarely, if ever, read the terms and conditions or privacy statements.[109] In most cases he or she "clicks" and "accepts" and then moves on to the services.[110] These terms and conditions only come to the light of day when there are news reports that, for example, an email provider or a social network provider changed its privacy policy.[111] Google and Facebook are often the wrath of backlash when they openly and honestly let users know of changes.[112] When Google

---

[107] *See Microsoft Privacy Statement*, MICROSOFT (Sept. 2016), *archived at* https://perma.cc/G6XU-UA9W (explaining the reasons why Microsoft controls personal data).

[108] *See id.* (explaining Microsoft's cooperation with law enforcement).

[109] *See, e.g.*, Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contracts: Lessons and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP.1, 21 (2009) (citing the FTC notion that consumers don't read, or find it difficult to read privacy agreements and terms and conditions online).

[110] *See Create an Account*, MICROSOFT (Oct. 25, 2016), *archived at* https://perma.cc/W56G-PAS2 (stating that "clicking create account means that you agree to the Microsoft Services Agreement and privacy and cookies statement"). When signing up for a Microsoft account, a user having filled in the relevant information, is instructed to "click create account to agree to the Microsoft Services Agreement and privacy and cookies statement," and these are provided in hyperlinks so that the reader can see all the terms and conditions. *Id.*

[111] *See* Tomio Geron, *After Backlash, Instagram Changes Back to Original Terms of Service*, FORBES (Dec. 20, 2012), *archived at* https://perma.cc/G6RE-MF8G (discussing the backlash social media providers face when they change their terms of services and conditions).

[112] *See* Lee Munson, *Facebook's got a new privacy policy, and it plans to share your data with partners*, SOPHOS (Feb. 2, 2015), *archived at* https://perma.cc/55JT-

unified its terms and conditions in recent years and made such unification applicable to all its services it faced harsh criticisms.[113]

Microsoft has recently unified its privacy policy that applies to the Windows services but faced little or no criticisms.[114] In broad terms, the need for privacy or protection of personal internet data and to comply with modern laws on data grabbing/retention reflects that online privacy requires some form of trade-offs,[115] and such tradeoffs, may result in an abuse, as opposed to positive tradeoffs.[116] The bone of contention in the *Microsoft Search Warrant* was that of personal internet data located in Ireland.[117] But Microsoft has a global and uniform privacy policy and it states that it may cooperate in good faith to release such information to law enforcement agencies.[118]

When creating an account for Microsoft Services, the Microsoft Services Agreement[119] and Microsoft's Privacy and Cookie Statements[120] are essential to the legal nature of the account the user creates.[121] These legal documents shield the service provider from liabilities and also instruct the user that his or her data may be handed

---

CV7A (stating how Facebook users are upset with the new change in terms and conditions).

[113] *See* Gordon Kelly, *Private Property: What Google's Unified Privacy Policy Means for You*, ITPROPORTAL (Feb. 14, 2012), *archived at* https://perma.cc/AA97-QBGW (outlining the ramifications of Google's unified privacy policy).

[114] *See Microsoft MSA*, *supra* note 44 (highlighting the unified privacy policy of Microsoft).

[115] *See* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221 (2016) (discussing governmental threats to privacy).

[116] See Miller, *supra* note 1, at 43 (discussing the abuse that can occur when these tradeoffs take place).

[117] *See* Microsoft Search Warrant, 15 F. Supp. 3d at 466 (reiterating the main issue in the case).

[118] *See Microsoft Privacy Statement*, *supra* note 107, at 5 (discussing when Microsoft is required to release information).

[119] *See Microsoft MSA*, *supra* note 44 (displaying the Microsoft Service Agreement for users to view).

[120] *See Microsoft Privacy Statement*, *supra* note 107 (setting out Microsoft's privacy policy, including a provision discussing "cookies").

[121] *See Microsoft MSA*, *supra* note 44 (explaining potential consequences of violating the agreement); *see also Microsoft Privacy Statement*, *supra* note 107 (discussing the framework of how and when data is collected and released).

over to law enforcement agencies.[122] Furthermore, as private actors, Internet communication providers such as Microsoft have international obligations under international instruments such as UN Guiding Principles[123] and MLATs to act in conformity with international law.[124] Although, the UN Guiding principle is a soft law instrument, it goes to show that more legislative activity at the global level is needed.[125] But, so far, the main question as raised in the *Microsoft Search Warrant (2014)* decision, and also during the appeals process that resulted in a second circuit decision in 2016, is the application of domestic law extraterritorially.[126] That legislation in question is the Stored Communication Act ("SCA") and its relation to MLATs.[127]

IV. Data Retention, Mutual Legal Assistance and the SCA Before and During the Internet Era

Because the data in question in *Microsoft Search Warrant* resides in Ireland, which is the European "offshore hub" for Silicon Valley companies, and is protected by EU and Irish data protection laws, both the U.S. Government and the Courts were asking Microsoft to break those laws and also to provide a sovereignty backdoor access to Ireland on behalf of the United States.[128] From this

---

[122] *See Microsoft MSA*, *supra* note 44 (setting forth dispute resolution procedures); *see also Microsoft Privacy Statement*, *supra* note 107 (listing instances where data can be released to third parties).

[123] *See* Nicola Jägers, *UN Guiding Principles on Business and Human Rights: Making Headway towards Real Corporate Accountability*, 29 NETH. Q. HUM. RTS. 159, 159 (2011) (articulating the importance and purpose of the U.N. guiding principles).

[124] *See* U.N. Secretary-General, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 1, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) (recognizing the history and purpose of necessity for the Guiding Principles as a model for international law).

[125] *See id.* at 9 (outlining the importance of the Guiding Principles and stating the need for continued cooperation from Governments).

[126] *See* Microsoft Corp v. United States, 829 F.3d at 209 (analyzing the application and the enforcement of domestic law extraterritorially).

[127] *See id.* at 210 (highlighting the issues of the SCA as applied outside the United States).

[128] *See* Ryngaert, *supra* note 8, at 222 (stating that U.S. e-discovery orders from U.S. corporations in regards to data held on foreign servers generates conflict in international law.)

point of view the U.S. government was essentially asking Microsoft to be an *evil agent,* thus forcing a transnational corporation to *commit crimes against privacy* on behalf of the U.S Government.[129] For Microsoft the consequences could be harsh, as it likely would have faced being dragged before Irish and European Courts for breaches of data protection rules and also face significant financial fines for breaching those rules and breaching the trust and sanctity of its customers.[130] One interesting argument the government raised in the *Microsoft Search Warrant* case was comparing the obligation of Microsoft to transfer the data requested similar to the obligation of paying taxes: "the fact that a corporation may need to move funds from a foreign bank account into the United States in order to pay its taxes, due to the corporation's own banking practices, does not render the tax laws 'extraterritorial.'"[131] But this misses the point, and moreover, there are dozens of bilateral tax treaties with the U.S. and other countries that fill the gap and would not need the extraterritorial application of U.S. tax laws.[132] However, the piece of legislation in question that the government argued that obliges Microsoft to transfer the requested data, the SCA, as it is seen as a data grabbing legislation can generally be counted as "evil."[133]

---

[129] *See id*. at 223 (stating that "[u]nderneath the jurisdictional discourse, dominated by such concepts as
territoriality, effects, and personality, lies a more substantive discourse regarding the appropriate balance
to be struck between data protection and other societal goals, such as security").
[130] *See* Bradley S. Shear, *Microsoft Search Warrant Case is a Win for Privacy*, LAW360 (July 22, 2016), *archived at* https://perma.cc/PZE7-8YXY (illustrating how the U.S. government tried to circumvent international privacy law utilizing the SCA).
[131] Brief of Government in Support of Magistrate's Decision, *supra* note 102, at 19.
[132] *See United States Income Tax Treaties – A to Z*, INTERNAL REVENUE SERVICE (Feb. 22, 2016), *archived at* https://perma.cc/75EW-XESF (stating that the United States has numerous tax treaties with foreign countries).
[133] *See Microsoft Corp*., 829 F.3d at 212 (inferring that the law requiring Microsoft to turn over data is the same type of "evil" that the Fourth Amendment was supposed to protect against).

But is Microsoft bound to handover the data? By its own acknowledgement in the MSA, that is a "yes" so then, why the resistance?[134] Part of the answer lies in Microsoft not wanting to breach EU data protection rules and also treating the requested data as property.[135] If one is to treat the data as any other form of property, including physical property, then there are reasonable grounds that although Microsoft controls and can access the data it must proceed cautiously.[136] In *United States v. Verdugo-Urquidez*,[137] the U.S. Supreme Court concluded that Fourth Amendment does not apply to the search and seizure of property owned by non-resident alien and located in a foreign location.[138]

Under these circumstances, the issue is no longer purely a domestic concern, but a concern to sovereignty, international law, and the extraterritorial application of U.S. laws.[139] To be fair, that issue was addressed by the government in the *Microsoft Search Warrant*, and the government noted that the presumption of extraterritoriality did not apply "because the SCA warrant at issue does not involve any 'extraterritorial application' of U.S. law."[140] However, in other cases, such as those involving the terrorist bombing of embassies in Africa, the Government made it clear that there was no need for search warrant to carry out overseas search of premises, since those searches were "reasonable."[141]

---

[134] *See Microsoft Privacy Statement*, *supra* note 107 (exemplifying Microsoft privacy agreement when data is turned over to law enforcement).
[135] *See Microsoft Search Warrant*, 15 F. Supp. 3d at 470 (noting the simplicity of Microsoft's argument that federal courts cannot issue warrants to seize property outside of the United States).
[136] *See* John N. Love & Ann F. Ketchen, *Physical But Not Tangible: Electronic Data Losses*, LAW360 (Nov. 30, 2010), *archived at* https://perma.cc/VD28-RV25 (detailing the extent that courts have recognized data as physical property).
[137] 494 U.S. 259 (1990).
[138] *See id.* at 259 (explaining the court's holding the Fourth Amendment does not apply to property owned by a non-resident alien or located in a foreign nation).
[139] *See id.* at 267-68 (describing Fourth Amendment's history as applied to international law).
[140] Brief of Government in Support of Magistrate's Decision, *supra* note 102, at 18.
[141] *See* United States v. Odeh (In re Terrorist Bombings of United States Embassies in E. Afr.), 552 F.3d 157, 174 (2008) (discussing why intrusion into defendant's house was reasonable and balanced against the need for the government to monitor the activities of Al Qaeda).

The SCA,[142] enacted as part of the Electronic Communications Privacy Act of 1986 ("ECPA"),[143] allows the U.S. government full access to electronic communications and data.[144] The SCA covers in particular electronic communication services ("ECS"), remote computing services ("RCS"),[145] and the providers of emails and other internet communication companies such as those commonly used for social networking falls into the broad definition of public providers of electronic communication under the SCA.[146] The definitions of ECS and RCS under the SCA are rather broad and blurry and therefore both emails and other digital footprints of an individual and the service providers and hosting facilities can fall within the broad definitions under the SCA.[147]

The broad definitions of RCS and ECS under the SCA thus give significant leverage to law enforcement agencies to classify for example, Microsoft, Google, Twitter, and Facebook among others as both RCS and enabler of ECS.[148] Furthermore, these companies are significant examples because they are American and despite significant overseas operations, their central servers allow for the transmission of data located overseas to invariably pass through or be stored

---

[142] *See* 18 U.S.C. §§ 2701-2712 (2012) (listing the range of sections included in the Stored Wire and Electronic Communications and Transactional Records Access Act).

[143] *See* 18 U.S.C. §§ 2510-2522 (1986)*; see also* Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 268 (2013) (explaining the concern that the Electronic Communications Privacy Act did not fully protect privacy at the time); Orin Kerr, *The Next Generation Communications Privacy Act,* 162 U. PA. L. REV. 373, 373 (2014) (stating that Congress enacted the ECPA in 1986).

[144] *See* 18 U.S.C. §§ 2510–2522 (declaring it lawful to access electronic communications).

[145] *See* 18 U.S.C. § 2711(2) (defining the term "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system").

[146] *See* 18 U.S.C. § 2510(15) (defining the term "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

[147] *See* 18 U.S.C. § 2703 (discussing the federal requirements of disclosures of customer communications or records).

[148] *See* 18 U.S.C. §§ 2701-2712 (setting out broad definitions to terms referenced in the statute).

to headquarters servers.[149] At least Microsoft in its instructions for residents of the European Union states who sign up to its services informs them that their data is stored on U.S. servers in Washington State: "Your account information is stored on Microsoft servers located at One Microsoft Way, Redmond, Washington 98052 USA."[150]

The U.S., has in the past, contended that its laws can be applied extraterritorially,[151] and there is nothing preventing the U.S. from doing so in cases where there is a perceived "national security threat" that may emanate from the personal digital contents of a non-resident alien in a locality overseas where data protection laws are stronger than that of the U.S.[152] Thus, despite the presumption of extraterritoriality, if personal digital content located overseas presents a national security threat to the U.S. and "Congress has indicated its intent to reach such conduct, a United States court is bound to follow the congressional direction."[153] In *Yousef*, the United States Supreme Court explained that "the presumption against extraterritorial application does not apply to those criminal statutes which are, as a class, not logically depended on their locality for the Government's jurisdiction (*internal quotations omitted*)."[154] In addition to the SCA, other legal methods exists for which the U.S. engages in data grabbing techniques, and these include through the Foreign Intelligence Surveillance Act ("FISA")[155] which allows the U.S. government to

---

[149] *See About Your Privacy Rights*, MICROSOFT (Apr. 28, 2016), *archived at* https://perma.cc/QCQ3-HAGU (informing users where their data is stored).
[150] *See id.* (explaining that data is stored at One Microsoft Way, Redmond, Washington 98052 USA).
[151] *See* Equal Employment Opportunity Commission v. Arabian American Oil Co., 499 U.S. 244, 248 (1991) (mentioning that U.S. laws previously applied extraterritorially).
[152] *See* Laurie T. Lee, *The USA Patriot Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUT. & TECH. L. REV. 371, 372 (2003) (discussing the impact of the Patriot Act on Internet Service Providers).
[153] *See* United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003) (discussing applicable United States law to extraterritorial conduct).
[154] *See id*. (noting how extraterritorial application may apply in criminal cases).
[155] *See* 50 U.S.C. § 1801 (2015) (defining foreign intelligence information and its application).

obtain ex parte judicial orders authorizing domestic electronic surveillance and also indirectly through MLATs.[156]

The MLATs treaties are rather silent on the nature of data as part of the cooperation obligations between states.[157] This makes the issue all the more problematic for international law and reveals its troubled state and inability to respond to issues that touch upon the lives of global citizens.[158] In fact, some countries are applying similar data grabbing laws, such as the SCA, and for example, the Investigatory Powers Act 2016 in the U.K., often dubbed the snoopers charter. The Investigatory Powers Act of 2016 requires internet service providers to retain private internet communications for twelve months,[159] allows government access to bulk data,[160] and crucially, can be enforced against overseas companies.[161] In short, the Investigatory Powers Act 2016 is a legal route that allows the UK, instead of applying its laws extraterritorially, shields the UK from any hacking

---

[156] *See id.* (defining key terms of the Foreign Intelligence Surveillance Act)*; see also* James G. McAdams, *Foreign Intelligence Surveillance Act (FISA): An Overview*, FEDERAL LAW ENFORCEMENT TRAINING CENTER, *archived at* https://perma.cc/3JEP-VX3P (explaining how FISA helps the United States government obtain information via domestic surveillance); Carl D. Giesy, *Jurisdictional Limitations on the Foreign Intelligence Surveillance Court*, 8 Suffolk Transnat'l L.J. 259, 290 (1984) (discussing electronic surveillance under the FISA).

[157] *See* Anna-Maria Osula, *Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data*, 9 Masaryk U. J.L. & Tech. 43, 2015 (discussing states needs for effective means of trans-border data access). David Kris, *Preliminary Thoughts on Cross-Border Data Requests*, LAWFARE (Sept. 28, 2015), *archived at* https://perma.cc/J7TP-QMP3 (showing the few specific cases that have ruled on United States and foreign government collaboration).

[158] *See* Kris, *supra* note 157(outlining the difficulties that foreign governments and the United States face in data production).

[159] *See Investigatory Powers Act 2016: Chapter 25*, *supra* note 25, at 33 (stating in Part 4, Paragraph 87(iii) that there are safeguards in place for the misuse of surveilled information).

[160] *See Investigatory Powers Act 2016: Chapter 25*, *supra* note 25, at 4-5 (discussing the Foreign Secretary's request for bi-yearly inspections of Bulk Personal Databases).

[161] *See Investigatory Powers Act 2016: Chapter 25*, *supra* note 25, at 36 (explaining that safeguards will not apply to certain partners with whom the SIA shares data).

it conducts beyond its borders, or what the Act refers to as "equipment interference."[162]

In the *Microsoft Search Warrant* decision the fundamental issue at its heart is that of jurisdiction and extraterritoriality.[163] But because the case involves the United States and Ireland (and the laws of the EU from a broader scope), one particular piece of international treaty is relevant to assess.[164] Ireland, like most of the EU and other countries in the world, signed bilateral treaties with the U.S. for cooperation in criminal matters.[165] The MLATs generally impose obligations on the parties to provide "specific categories of assistance" typically in a criminal investigation.[166] But the MLAT in question here between the U.S. and Ireland is rather empty when it comes to the exchange of data per se, and because of this vagueness or lack of treaty language expressing such cooperation, then arguably, the states can compensate for this vagueness in the U.S.-Ireland MLAT by cooperating through good faith.[167] Article 17 of the U.S.-Irish MLAT

---

[162] *See Investigatory Powers Act 2016: Chapter 25*, *supra* note 25, at 57 (noting the possibility of the government obtaining information as a result of "equipment interference").

[163] *See Microsoft Corp.*, 829 F.3d at 226 (indicating that multijurisdictional issues make it difficult to determine whether a proposed application should be domestic or extraterritorial).

[164] *See id.* at 221 (addressing conflicting statutes between two countries concerning stored data).

[165] *See* Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, Ir.-U.S., Jan. 18, 2001, T.I.A.S. No. 13,137 [hereinafter Treaty Between the United States of America and Ireland] (setting forth an agreement between the United States and Ireland to share specific data related to criminal matters).

[166] *See* Eugene Solomonov, *U.S.-Russian Mutual Legal Assistance Treaty: Is There a Way to Control Russian Organized Crime?*, 23 FORDHAM INT'L L.J. 165, 199-200 (1999) (noting that MLATs typically identify specific areas where the parties intend to cooperate).

[167] *See* Treaty Between the United States of America and Ireland, *supra* note 165 (referencing the lack of provisions governing the exchange of data between the countries); Jonah F. Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARVARD NATIONAL SECURITY JOURNAL (Jan. 28, 2015), *archived at* https://perma.cc/QD7R-FCFL (arguing law enforcement agencies should use the MLAT process in good faith before seeking direct access to data).

merely states a range of options for which the parties can cooperate.[168]

The principle of good faith is well established practice in international law, and given the vagueness in the U.S.-Irish MLAT on electronic communications either state can in good faith acquiesce to an MLAT request for private data.[169] Some countries such as the U.K., which has a MLAT with the U.S. instructs its prosecution service to also request "computer evidence" when making requests under the MLAT.[170] But even if states do not in good faith disclose requested information via MLAT channel, if such information concerns a private individual, then either party can turn to the terms of the MLAT to argue that a "private person" cannot suppress the disclosure of such data.[171] Thus, for example, in *Microsoft Search Warrant* decision the individual in question cannot rely on his individual rights

---

[168] *See* Treaty Between the United States of America and Ireland, *supra* note 165 (highlighting the different methods of cooperation available to the parties). The treaty includes the following language:

> Assistance and procedures set forth in this Treaty shall not prevent either Party from granting assistance to the other Part through the provisions of other applicable international agreements, or through the provisions of its national laws. The Parties may also provide assistance pursuant to any bilateral arrangement, agreement, or practice which may be applicable.

Id.

[169] *See* Treaty Between the United States of America and Ireland, *supra* note 165 (observing the absence of provisions related to administering requests for data in the treaty)*; see also* Steven Reinhold, *Good Faith in International Law*, 2 UCL J. L. & JURISPRUDENCE 40, 41 (2013) (establishing that the good faith principle is internationally recognized).

[170] *See Disclosure of Material to Third Parties*, THE CROWN PROSECUTION SERVICE, *archived at* https://perma.cc/PG6L-CK4S (outlining the different principles by which third parties can make evidentiary requests)*; see also* United States v. Moloney (In re Price), 685 F.3d 1, 9-10 (1st Cir. 2012), *cert. denied* 133 S. Ct. 1796 (2013) [hereinafter *In re Dolours Price*] (referencing a formal request for information under an MLAT for legal assistance in a pending criminal investigation).

[171] *See* Robert N. Lyman, *Compulsory Process in a Globalized Era: Defendant Access to Mutual Legal Assistance Treaties*, 47 VA. J. INT'L L. 261, 288-89 (2006) (summarizing rights of private parties under negotiated MLATs).

to squash a request made by the U.S. government to the Irish government.[172] This is clearly evident from the U.S.-Irish MLAT treaty language: "This 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 exclude *any evidence, or to impede the executive of a request*" (emphasis added).[173]

From a reading of this provision then, it is clear that MLATs can serve effectively the purposes of the request to hand over personal email contents, and in doing so exclude the rights of private individuals, which they consented to while registering for Microsoft Services.[174] U.S. Courts are known to deny private rights that presumably arose out of MLAT treaties.[175] For instance, in the *Dolours Price* decision,[176] the Court ruled that the U.S.-U.K. MLAT did not give any rise to a private action to torpedo a subpoena.[177]

So in one sense, Microsoft's resistance to hand over personal internet data is laudable, but at the same time it faces legal obstacles, and because it warns users that they may hand over data when re-

---

[172] *See Microsoft Corp*., 829 F.3d at 221 (limiting privacy rights as a defense against extraterritorial warrants).

[173] *See* Treaty Between the United States of America and Ireland, *supra* note 165, at 2 (clarifying party intentions for private individual rights under the treaty).

[174] *See* Treaty Between the United States of America and Ireland, *supra* note 165, at 2 (inferring extraterritorial rights to data requests under the treaty); *see also Microsoft MSA*, *supra* note 44 (contending private individuals waive their rights through consenting to the Microsoft Terms of Use); Michael J. Dunne & Anna L. Musacchio, *Jurisdiction Over the Internet*, 54 BUS. LAW. 385, 398-400 (1999) (discussing jurisdiction in relation to "foreign located entities"); J. Christopher Gooch, *The Internet, Personal Jurisdiction, and the Federal Long-Arm Statute: Rethinking the Concept of Jurisdiction*, 15 ARIZ. J. INT'L & COMP. L. 635 (1998).

[175] *See In re Dolours Price*, 685 F.3d at 9 (holding that the appellants failed to advance private right's claim under the MLAT); In re Grand Jury Subpoena, 646 F.3d 159, 165 (4th Cir. 2011) (denying the company's argument to allow private rights under MLAT); United States v. Chitron Elecs. Co., 668 F. Supp. 2d 298, 306-07 (D. Mass. 2009) (enforcing the lack of private right in MLAT treaty).

[176] *See In re Dolours Price*, 685 F.3d at 6 (discussing the US-UK MLAT Subpoenas).

[177] *See id.* at 9 (rejecting the appellant's MLAT claim of private action).

quested, it appears that the resistance is only to build users' confidence.[178] The data requested under the warrant in the *Microsoft Search Warrant* decision can be transferred overseas or outside of the EEA to the U.S. through the EU-U.S. safe harbor provisions or via the U.S.-Irish MLAT.[179] The safe harbor provision are a set of principles that companies subscribed to and are considered to have met EU standards on data protection.[180] The EU's data protection regime, although it is undergoing revision, has become the *de-facto* international legal regime for privacy and data protection.[181] The information privacy laws at the *supra-federal* Europe also once had a data retention legislation,[182] and when it is compared to Stored Communication Act, it too is quite troublesome.[183]

The Data Retention Directive had been quite a thorn in the side of privacy activists and moreover, prior to the CJEU ruling in April 2014 declaring the Data Retention Directive invalid,[184] it had

---

[178] *See Microsoft Corp.*, 829 F.3d at 221 (referring to Microsoft's refusal to provide data stored in Ireland)*; see also Microsoft Privacy Statement*, *supra* note 107 (noting Microsoft's ability providing data to law enforcement under the privacy statement).

[179] *See* Barbara C. George et al., Article, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 739 (2001) (articulating the applicability of Safe Harbor Principles to transatlantic data flow).

[180] *See id.* at 749-50 (explaining the rationale behind the EU data privacy directive and the need for US employers to comply).

[181] *See* Nora Ni Loidean, *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*, 19 NO. 8 J. INTERNET L. 1, 12-13 (2016) (stating that although the effects of the standards have yet to be realized, most EU countries have been implementing them).

[182] *See* Council Directive 2006/24/EC, 2006 O.J. (L 105) 54 (EC) [hereinafter the Data Retention Directive] (establishing new data retention initiative); *see also* Ni Loidean, *supra* note 181, at 9 (signifying the creation of the EU Data Retention Directive).

[183] *See* Elise M. Simbro, Note, *Disclosing Stored Communication Data to Fight Crime: The U.S. and EU Approaches to Balancing Competing Privacy and Security Interests*, 43 CORNELL INT'L L.J 585, 596 (2010) (highlighting the issues in obtaining cell phone records under the Stored Communications Act).

[184] *See* Case C-293/12, Digital Rights Ireland Ltd. v. Minister for Communications, 2014 E.C.R. I-238 (overturning the Data Retention Directive). This matter was joined with Case C-594/12, Kärntner Landesregierung. *Id.*

been "invading" so to speak, the supposedly "good-guy" data protection directive space.[185] The Data Retention Directive was no different from the SCA in that it required a mandatory retention of data used for communication purposes, in particular data processed over the Internet.[186] Because the CJEU ruling declared the DRD invalid from the day it was entered into force, effectively wiping its footprints from the history books, the discussion in the next few paragraphs is based on the DRD as it existed before the court's ruling.

The Data Retention Directive entered into force in 2006 and its remit was to provide a harmonized method for EU Member states to retain electronic data and make it "available for the purpose of the investigation, detection and prosecution of serious crime."[187] The burden shifts to the providers of both electronic communications services[188] and public communications network[189] to retain certain data.[190] But the Data Retention Directive was always a hard sell to the general public and moreover the Data Retention Directive was seemingly at odds with that of data protection.[191] When the CJEU heard the complaint of Ireland and others on the scope of the DRD and gave its ruling in 2014, the court argued that the DRD exceeded

---

[185] *See* Elitsa Stoeva, *The Data Retention Directive and the Right to Privacy*, 15:4 ERA FORUM 575, 576 (Jan. 23, 2015) (expounding on the overreaching nature of the Data Retention Directive).

[186] *See* Data Retention Directive, *supra* note 182, at 59 (requiring member states to retain data in such a way that it can be promptly provided to authorities); *see also* 18 U.S.C. § 2704 (mandating the retention of communication procedures).

[187] *See* Stoeva, *supra* note 185, at 580 (explaining how the Data Retention Directive assisted in retention and prosecuting serious crimes).

[188] *See* Stoeva, *supra* note 185, at 582 (illustrating the obligation of the electronic communications services to retain data).

[189] *See* Stoeva, *supra* note 185, at 576 (highlighting the obligation of the public communications networks).

[190] *See* Data Retention Directive, *supra* note 182, at 9 (defining who has the obligation to retain data).

[191] *See* Mirko Hohmann, *German Bundestag Passes New Data Retention Law*, LAWFARE (Oct. 16, 2015), *archived at* https://perma.cc/WE5S-4YCQ (inferring that Data Retention Directive is an infringement of rights without a guarantee of effectiveness).

fundamental rights relating to privacy and data protection.[192] According to the CJEU, the DRD went over the board to the point there was no justified level of proportionate interference with the right to privacy and data protection:

> [The Data Retention Directive] does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Article 7 and 8 of the Charter [of Fundamental Rights of the European Union]. It must therefore be held that [the Data Retention Directive] entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.[193]

Now one could make the argument that given the Snowden effect that has been made public almost a year to the ruling, Europeans and by extension the Court were more willing to listen to those voices that opposed the DRD from the beginning.[194] But, whether or not this argument can hold is another matter. What is however certain is that the DRD and its SCA like provisions were "unconstitutional" in Europe and as such, unlike the SCA, its implementation and effect during its "lifetime" has been wiped from the pages of history, or until a replacement legislation is implemented in the EU.[195]

---

[192] *See European Union: ECJ Invalidates Data Retention Directive,* LIBRARY OF CONGRESS, *archived at* https://perma.cc/BW9L-WFH6 (discussing that the High Court in Ireland's finding was that the Data Retention Directive violates privacy).
[193] *See Digital Rights of Ireland Ltd.*, 2014 E.C.R. at I-238 (discussing how Directive 2006/24 encompasses a serious interference with civil rights under the laws of the European Union).
[194] *See How Digital Rights Ireland Litigated Against the EU Data Retention Directive and Won*, ELECTRONIC FRONTIER FOUNDATION, *archived at* https://perma.cc/75WD-KLPB (describing the shift in the political climate which now opposes the Data Retention Directive of the EU).
[195] *See Digital Rights of Ireland Ltd.*, 2014 E.C.R. at I-238 (inferring what replacement legislation should entail in order to be constitutional).

The ruling by the CJEU was not surprising and it was long in the making,[196] as a result of the many opposition the DRD faced. The actual surprising detail about the ruling was that the CJEU finally cemented itself as a reviewer of legislations in Europe's constitutional quest, and on this occasion it was able to find one of those legislations as "unconstitutional."[197] But this finding also gives the European legislative and decision making processes a good chance for replacing the DRD with a more functional data retention regime that at least does not infringe on those fundamental rights such as that of data protection and the right to privacy.[198] But even if a more functional data retention regime is put in place there is still the problem of data grabbing techniques that either firms or governments can use to acquire data that electronic service providers and communications companies transmit or stores on their internal servers.[199] Moreover, under such circumstances, some states would want to access that data using their national laws and through MLATs, in particular, if they argue that a threat exist to their national security and accessing that data can thwart the threat.[200] This brings the discussion back to the *Microsoft Search Warrant* decision.[201]

Although the decision was at the district court level, it reverberates through all hall of justices in the US. Furthermore, from an international law perspective, the central issue is that of jurisdiction, because Microsoft was ordered to comply with a search warrant to reveal the personal internet data in connection with an email account

---

[196] *See Report from the Commission to the Council and the European Parliament*, at 2, COM (Apr. 18, 2011) (describing the extensive discussions that went into the creation of this report).

[197] *See id.* at 32 (ensuring that there will be more consistency in reviewing the EU data protection framework).

[198] *See id.* at 28 (explaining that the European Union uses DRD principles in its approach to data retention in order to protect the fundamental rights and freedoms of others).

[199] *See Data Retention*, ELECTRONIC PRIVACY INFORMATION CENTER, *archived at* https://perma.cc/DA9G-SZ2D (clarifying the potential problems that may arise, such as DRD having negative repercussions on citizens of other countries or non-government law enforcement agencies).

[200] *See id.* (stating that according to the laws of national security, nations whose national security is at risk may be allowed access to the retained data).

[201] *See Microsoft Search Warrant*, 15 F. Supp. 3d at 466 (discussing the search and seizure of electronic information).

hosted in Ireland.[202] There are a number of questions that can be explored further.[203] Does the U.S. have the right to *invade* the sovereignty of another state where stronger data protection laws exists, and where that state is part of a *supra-federal* legal system under international law?[204] Clearly, the answer is no, but this does not mean that there is a clear cut way at reaching this answer under international law.[205] At the heart of the issue is that of jurisdiction – one of the most troublesome areas under international law.[206] The question of jurisdiction is troublesome in this context because it juxtaposes the clash of two legal cultures: a civil-Romano legal culture widely practiced in most part of the world and the Common law legal culture predominant in Anglo-American law. [207] The clash of the two legal cultures and their approach and interpretation of jurisdictional problems in international law may suggest that the Anglo-American common law interpretation is more superior, which also has a history of applying its laws extraterritorially.[208] For information privacy laws, the question of jurisdiction is even more troublesome, when the vague message of the European Data Protection regime is taken into consideration, where, according to the DPD, by virtue of public international law, national law is applicable under certain circumstances when processing personal data.[209]

---

[202] *See id.* (summarizing that Microsoft was ordered to reveal information).
[203] *See* Brown & Korff, *supra* note 89, at 4 (examining questions related to international law requirements on the right to invade).
[204] *See* Brown & Korff, *supra* note 89, at 43 (explaining that it is a violation of sovereignty to demand access to data extraterritorially).
[205] *See* Brown & Korff, *supra* note 89, at 4 (showing how bypassing the "Mutual Legal Assistance Treaties" constitutes an infringement of sovereignty).
[206] *See* Brown, *supra* note 89, at 4 (illustrating the difficulties of government agencies obtaining information from outside of their jurisdiction).
[207] *See* Richard Ford, *Law's Territory*, 97 MICH. L. REV. 843, 904 (1999) (juxtaposing territorial and non-territorial jurisdictions).
[208] *See* Daskal, *supra* note 8, at 383 (exemplifying the presumption that U.S. law applies outside of U.S. jurisdiction).
[209] *See* Data Protection Directive, *supra* note 182 (stating that "the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law").

So how does one go about resolving the problem of jurisdiction in matters such as the *Microsoft Search Warrant* decision regarding the email and personal internet data located in Ireland? To do that, we need to answer a basic question: Can U.S. laws be applied extraterritorially to data located overseas?

Judging by the last decision when the U.S. Supreme Court faced with a similar question – the answer is "no" because the Court in *Kiobel v. Royal Dutch Petroleum Co.*[210] was rather succinct: "when a statute gives no clear indication of an extraterritorial application, it has none."[211] But despite this pronunciation from the U.S. Supreme Court, had the *Microsoft Search Warrant* decision reached its judicial halls, it is likely that the Court could overturn itself because one possible argument of the government could have been the nature of national security, where rulings such as *Kiobel* on extraterritoriality would not have applied because they do not deal with "national security."[212] This is important because the blanket coverage of "national security" generally favors governments in their pursuit of terrorist and other criminal activities – especially on terrorism-related allegations where the state exercises control to the point that it can sanction indefinite retention without trial under the rubric of national security.[213]

In fact, the Russian Data Retention law of 2016, is in part, based on national security grounds in relation to "terrorism".[214] But in the case of the US, the U.S. Supreme Court could look to precedent elsewhere, such as in wiretapping to argue that to prevent criminal enterprise from flourishing that could harm national security, the country's access to remotely held data is necessary.[215] At least in

---

[210] 133 S. Ct. 1659 (2013).

[211] *See id.* at 1664 (2013) (referencing extraterritorial test set out by the *Morrison* court).

[212] *See id.* at 1673 (Thomas, J., concurring) (inferring that the majority's holding hinged on the issue of national security).

[213] *See* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 697 (2004) (discussing the court's flexibility with government actions in cases concerning decisions of national security).

[214] See Melnlkova, *supra* note 25 (noting that Yarovaya Law "makes it a crime not to report information about terrorist attacks").

[215] *See Prepared Opening Remarks of Attorney General Alberto R. Gonzales at the Justice Department Oversight Hearing of Senate Judiciary Committee*, UNITED

Olmstead v. United States,[216] the U.S. Supreme Court upheld the government's telephone wiretapping program could influence such an argument if criminal enterprising harms the national security of the nation.[217]

V. Should the SCA Be Given Extraterritorial Effect?

From the above analysis that discusses private data such as emails and financial records – the obvious question that remains in light of the SCA and the efforts by U.S. authorities to obtain private data located on overseas servers is whether the SCA should be applied extraterritorially. The U.S. has had a long history of applying domestic law extraterritorially, perhaps with antitrust laws[218] and securities laws being the most famous pieces of legislations that heads the extraterritorial application of U.S. domestic laws.[219] The SCA is only the latest U.S. legislation that has joined the list in which the U.S. government is attempting to apply beyond its own domestic shores.[220]

In recent cases such as *Morrison v. National Australia Bank*[221] the U.S. Supreme Court explained that U.S. laws are only to be applied in its territorial jurisdiction: "[the] longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of

---

STATES DEPARTMENT OF JUSTICE (Jan. 18, 2007), *archived at* https://perma.cc/UP46-SEVG (speaking generally about electronic surveillance programs).

[216] *See* Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967) (finding that the wiretap did not amount to a search or seizure).

[217] *See Olmstead*, 277 U.S. at 468-69 (holding that wiretapping conversations, obtained without judicial approval, violates the Fourth Amendment).

[218] *See* United States v. Aluminum Co. of America, 148 F.2d 416, 429 (2d Cir. 1945) (explaining that extraterritorial application of the law has been assumed).

[219] *See id.* at 439 (expanding upon the implications of using domestic law extraterritorially).

[220] *See* Stored Communications Act, 18 U.S.C. § 2711 (demonstrating the reach of the SCA).

[221] 561 U.S. 247 (2010).

the United States."[222] The SCA is one of those statutes that U.S. legislators have not given any expression of extraterritorial effect.[223]

In cases such as *Kiobel v. Shell*, the U.S. Supreme Court also warns of encroaching on the Sovereignty of a nation by interpreting U.S. law to have an extraterritorial effect.[224] According to the *Kiobel* Court, if there is no "clear indication of an extraterritorial application, then it has none," and as such, U.S. law does not rule the world, and therefore, unintended clashes and international discord with another nations should be avoided: "the danger of unwarranted judicial interference in the conduct of foreign policy [should be avoided] because the question is not what Congress has done but instead what courts may do."[225] Although the U.S. Supreme Court expresses clear language on the non-interference of sovereign nation's jurisdictions by using U.S. domestic laws – the Judge in *Microsoft Search Warrant* Case, on the other hand, believes that there is an exception for the SCA, given that he ruled in favor of such search warrants regarding data held on foreign servers.[226] The decision, was however, overturned by a Federal Court.[227]

In applying the reasoning of *Kiobel*, whereas the Courts are to be spared from making foreign policy intrusion as opposed to the U.S. Congress is quite worrisome.[228] The *Search Warrant* judgment makes it clear to the U.S. government that it can compel Internet communication companies to produce personal internet data stored overseas, but more so, that U.S. law should be given extraterritorial

---

[222] *See Morrison*, 561 U.S. at 255 (2010) (explaining that U.S. law is binding only in U.S. jurisdictions).
[223] *See* Stored Communications Act, 18 U.S.C. § 2711 (discussing the jurisdiction of the SCA).
[224] *See Kiobel*, 133 S. Ct. at 1664 (discussing the adverse effects of encroaching on other countries' jurisdictions).
[225] *Id.* (explaining the effects on foreign policy of extraterritorial interpretation).
[226] *See Microsoft Corp.*, 829 F.3d at 210 (clarifying that the SCA does not have extraterritorial effect).
[227] *See Microsoft Corp.*, 829 F.3d at 201 (reversing, vacating, and remanding the District Court's decisions).99
[228] *See Kiobel*, 133 S. Ct. at 1664 (noting the potential dangers of restricting the Courts, but not Congress of intruding on matters of foreign policy).

effect.[229] What makes the *Search Warrant* case even more worrisome beyond the problems of the extraterritorial application of U.S. law is the fact that the lower court reasoned that the search warrant is "hybrid" – part warrant and part subpoena.[230]

This is further disturbing because the district court cast a wide net to compel Microsoft to hand over the personal internet data – at all costs – so far as to reason that "all records or other information regarding the identification of the account" must be handed over. [231] The magistrate judge, by reasoning that "a subpoena requires the recipient to produce information its possession, custody, or control regardless of the location of that information," then suggests that U.S. law, specifically the SCA, has extraterritorial effect.[232] However, on appeal the Second Circuit viewed things differently and held that Congress did not have the intention for the SCA to have extraterritorial effect.[233]

VI. Conclusion

This article reveals that governments are the most prolific perpetrators of "war crimes" against privacy. If anything, that was the intended effect of the *Microsoft Search Warrant* decision in 2014. Even from a commercial perspective, governments often outmaneuver commercial operators and even intimidate commercial operators to the point of submission and cooperation through compliance of information privacy laws. If the continued "war against privacy" can be thwarted, it would require states to formulate a coordinated approach towards protecting privacy at the international level. It is troubling that U.S. laws, in some instances, are being still viewed as

---

[229] *See Microsoft Corp*., 829 F.3d at 204 (reiterating how the U.S. may force communication companies to produce data).
[230] *See id.* (explaining the magistrate judge's ruling that an SCA warrant is executed like a subpoena).
[231] *See id.* (setting forth the magistrate's conclusion).
[232] *See id.* (noting the trial court's reasoning that the place of review was the United States, but executing a warrant abroad was "not inconsistent with the statutory language").
[233] *See id.* at 222 (stating that the SCA was never intended to reach extraterritorial servers).

having extraterritorial effect, such as how the *Microsoft Search Warrant* case initially held. This was so, especially to confiscate personal internet data located overseas of foreign nationals, and this suggests that there is something inherently wrong with the status of information privacy laws both in the U.S. and at the international level.

It is quite clear that the issue of privacy is becoming a problem beyond the mere domestic laws of states. The issue has become a proverbial "hot-potato" in international legal relations and the challenge for states is how to respond with a coordinated approach to information privacy laws. A simple response would be for a global response to the problems of information privacy laws via the International Law Commission to convene a working group on the matter and study in particular state practices such as those in Europe, the Five Eyes Nations approach and propose actions and international treaties that can stir states into action to bring some form of unity to information privacy under international law. If international law is able spring into action and thwart the efforts of a few nations from single- handedly committing "war crimes" against privacy, then data protection and privacy would no longer be an emerging norm but a right that is shielded with international obligations.

There have been examples of calls for an international legal regime of data protection, and *ad hoc* groups such as the Privacy Commissioners have been leading that call. For instance, in one of their concluded sessions they noted that: "there is a pressing need for a binding international agreement on data protection that safeguards human rights by protecting privacy, personal data and the integrity of networks and enhances the transparency of data processing while striking the right balance in respect of security economic interests and freedom of expression."[234] This is only one step in the right direction.

The proliferation of data protection laws and data retention laws at the global level is contributing to the creation of global privacy information laws, and this new form of international legalism, although with different variations around the globe, is both welcome

---

[234] *Resolution on Anchoring Data Protection and the Protection of Privacy in International Law*, ORGANIZATION OF AMERICAN STATES, *archived at* https://perma.cc/7TVE-H3PW (stating what the 35th International Conference observed during prior meetings).

and at the same time troublesome. For instance, in the area of data retention laws, it has become even more troublesome, when nations such as the UK and Russia passed sweeping legislations on data retention that mixes terrorism, hacking and other forms of transnational issues as justification for such laws. On the other hand, in the area of data protection laws, the new international legalism is welcome because it edges towards a sort of constitutionalism of global information privacy laws where the liberty of the individual is central. There are interesting times ahead as the "war against privacy" moves into different directions and the ability of states to extend regulations into the digital jurisdiction and sovereignty of another country.