14-2985-cv

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION,

MICROSOFT CORPORATION,

Appellant,

—v.—

UNITED STATES OF AMERICA

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICI CURIAE* DIGITAL RIGHTS IRELAND LIMITED, LIBERTY, AND THE OPEN RIGHTS GROUP IN SUPPORT OF APPELLANT MICROSOFT CORPORATION

Edward McGarr
Simon McGarr
Dervila McGirr
MCGARR SOLICITORS
12 City Gate
Lr. Bridge St.
Dublin 8, Ireland

Owen C. Pell
Ian S. Forrester, Q.C.
Paige C. Spencer
WHITE & CASE
1155 Avenue of the Americas
New York, New York 10036
212-819-8891

Counsel for Amici Curiae Digital Rights Ireland Limited, Liberty, and the Open Rights Group

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* Digital Rights Ireland Limited, the National Council for Civil Liberties (known as "Liberty"), and the Open Rights Group each state that they have no parent corporations and that no publicly held company owns 10% or more of their respective stock.

WHITE & CASE LLP

By: /s/ Owen C. Pell
Owen C. Pell
Ian S. Forrester, Q.C.
Paige C. Spencer
1155 Avenue of the Americas
New York, New York 10036
Telephone: (212) 819-8200
Facsimile: (212) 354-8113

Counsel for Amici Curiae Digital Rights Ireland Limited, Liberty, and the Open Rights Group

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TREATIES AND STATUTES

MISCELLANEOUS

STATEMENT OF INTEREST OF THE AMICI CURIAE[1]

Digital Rights Ireland Limited ("DRI") is an Irish non-profit public interest organization committed to the protection of civil and political rights in the digital age. It has litigated before the European Court of Justice and elsewhere in a number of landmark cases on the status of digital rights. It favors consistent and predictable practices relating to the release of data to law enforcement authorities.

DRI is concerned about the legal, moral, and technical implications of a regime which, without regard to Irish regulatory or judicial oversight, would deliver to a U.S. prosecutor personal data that is located in Ireland. DRI believes that valid Irish jurisdictional concerns have been ignored in the U.S. proceedings thus far, notwithstanding the terms of a binding and self-executing treaty between the United States and European Union which provides for the balancing of Ireland's concerns with those of the United States through mutual legal assistance applications. The position of the United States would circumvent an existing treaty rendering it pointless, and violate important public policies embodied in the data privacy laws of Ireland.

Liberty, also known as the National Council for Civil Liberties, was founded in the United Kingdom 80 years ago. It campaigns for fundamental rights and

[1] This brief is filed with the written consent of all parties. No counsel for a party authored this brief in whole or in part, nor did any person or entity, other than *Amici* or its counsel, make a monetary contribution to the preparation or submission of this brief.

freedoms, and is dedicated to promoting the values of individual human dignity, equal treatment and fairness as the foundations of a democratic society. Among other things, Liberty campaigns to protect basic rights and freedoms through the courts. This includes bringing litigation against unnecessary state intrusion into people's personal lives, and to strengthen data privacy and protection under British and European law. Liberty is gravely concerned about the implications of the judgment under appeal. In an increasingly globalized world, Liberty appreciates how important it is that law enforcement should not be frustrated by issues of jurisdiction. But that is best achieved by mutual cooperation and respect for other legal systems and not through the unilateral assertion of jurisdiction.

The Open Rights Group ("ORG") is a non-profit company founded in 2005 by digital activists. ORG is one of the United Kingdom's most prominent voices defending freedom of expression, privacy, innovation, consumer rights and creativity on the Internet. It is currently supported by around 2,500 active supporters and is advised by a council of leading experts drawn from academia, media, the technology and entertainment industries and the legal profession.

ORG believes that people have the right to control their technology and data, and that strong data protection laws, including as established in the European Union, are an important part of preserving personal privacy rights. It believes that law enforcement agencies must be able to cooperate for the purpose of combatting

crime, and that such cooperation is in practice efficiently accomplished by using local law and international treaties such as the Mutual Legal Assistance Treaties at issue here. DRI, Liberty, and ORG have a substantial interest in this action because of the adverse precedent it could set with respect to the protections provided for data located in Ireland and Europe under Irish and European data protection and data privacy laws.

SUMMARY OF ARGUMENT

The United States seeks to compel Microsoft Corporation ("Microsoft") to produce in the United States email data stored in Ireland with a Microsoft subsidiary. The United States is ignoring a treaty designed to be self-executing whereby demands of this kind would be resolved using procedures established by the U.S. and Irish governments which were *created* precisely to balance the interests of the United States in law enforcement and of Ireland in data privacy. The treaty, the U.S.-Ireland Mutual Legal Assistance Treaty ("Irish MLAT") was ratified in connection with the U.S.-European Union Mutual Legal Assistance Treaty ("EU MLAT")[2] and *after* the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701-2712 (the "ECPA"), under which the U.S. government issued the warrant at issue here.

---

[2] See U.S.-Ireland Treaty on Mutual Legal Assistance, done Jan. 18, 2001, T.I.A.S. No. 13137 (2001); U.S.-European Union Agreement on Mutual Legal Assistance, done Jun. 23, 2003, T.I.A.S. No. 10-201.1 (2003). The Irish MLAT and EU MLAT are collectively referred to as "the MLATs."

Under Irish law the data content of the email account maintained in Ireland belongs to the author and owner of the account. That data may not be exported from Ireland by the Microsoft subsidiary which holds the data except in accord with Irish data privacy laws. The District Court, however, held that the United States could require Microsoft to deliver the email data notwithstanding Irish law and without using the Irish MLAT. This decision was wrong because:

1. No matter how the scope of U.S. jurisdiction is understood, it cannot be doubted that Ireland has jurisdiction over the data located in its territory, which data is subject to Irish law.

2. Ireland's interests in seeing its data privacy laws respected within its territory are significant and compelling. Vast amounts of electronic data are stored in datacenters around the world, and the volume of that data increases daily. Ireland has an exceptionally large number of datacenters. The individuals to whom that data belongs have entrusted the protection of that sensitive, intimate, personal information to the technology companies that own and operate those datacenters under Irish data privacy laws.

In Europe, the European Convention on Human Rights and the European Charter on Fundamental Rights recognize the importance of data protection as one of the fundamental values which a democratic society must uphold, and public anxiety about how personal data is held is very high. This is reflected in European

data protection legislation. It is a serious offence, with serious penalties, to transfer personal data to a country outside the European Union ("EU") absent assurance that standards for the protection of personal data are in place. The data content of the email account in issue is located in a datacenter in Dublin, Ireland. Under Irish and European Union law, that account and its management and administration are subject to the laws and regulations of its location. Nonetheless, the EU MLAT procedures now applied through the Irish MLAT would allow the United States to obtain the contents of the email account without offending the laws and sensitivities of Ireland.

3. The EU MLAT amended earlier MLATs, including the Irish MLAT, so as to address specifically issues of data privacy under EU law. In the EU MLAT, the United States recognized the importance of European data privacy laws *and* the need to balance those laws against the needs of law enforcement authorities to access data. Accordingly, the EU MLAT made clear that other than in exceptional circumstances data privacy laws could *not* be used to block a legitimate information request under an MLAT. The EU MLAT stated that the balancing of interests between U.S. and Irish law was to be accomplished through the MLAT information request process.

4. The United States expressly acknowledged that the EU MLAT was *self-executing*, would be read in conjunction with existing U.S. law, and required no

implementing legislation. As explained below, self-executing treaties are the exception rather than the rule, and create obligations enforceable under federal law. Self-executing treaties must be harmonized with existing federal law and given the fullest possible effect. As such, the obligation of the United States to use the MLAT procedures to balance U.S. law enforcement needs with Irish data privacy needs was dependent on the MLATs alone, and not any additional act of the U.S. Congress. Moreover, the EU MLAT was ratified by the United States in 2008 (with the Irish MLAT becoming effective in 2009), long after the ECPA provision at issue here, meaning that if the statute and the treaties could not be harmonized then any conflict between them must be resolved in favor of the MLATs.

5. By compelling Microsoft to produce protected data from Ireland via an ECPA warrant the District Court allowed the EU and Irish MLATs to be disregarded. This was an error for two reasons. *First*, the United States has chosen to read the MLATs as not constituting federal law that must be given effect. This, however, is expressly contrary to the self-executing nature of the MLATs, which the U.S. Senate said would "be implemented by the United States in conjunction with applicable federal statutes." Nothing about the U.S. position is *"in conjunction with"* existing law because the United States does not see the MLATs as having anything to do with its warrant power.

Second, the U.S. position reads the MLATs so narrowly as to render the EU and Irish MLATs superfluous. Rather than striving to read the MLATs in conjunction with the ECPA—as the Senate said would be done—the United States reads the MLATs as having no impact on existing U.S. law. But this crabbed reading of the MLATs effectively reads them out of existence.

Self-executing treaties create obligations. But, by compelling Microsoft to produce protected data from Ireland via an ECPA warrant, the District Court allowed the EU and Irish MLATs to be disregarded—i.e., treated as non-obligatory. The U.S. position that the MLATs are somehow not mandatory is precisely contrary to the concept of an obligation and so effectively renders the EU and Irish MLATs a nullity. Adopting the U.S. position would allow the U.S. government unilaterally to substitute U.S. court compulsion for the balancing process represented by the MLAT information request procedures. This destroys the self-executing nature of the MLATs by effectively holding that absent some further act of Congress to require their use—which the United States represented was not necessary—the MLAT procedures do not have to be used. This is contrary to law and precedent and should be reversed.

The United States and Ireland are two friendly democracies with a long history of cooperation and mutual understanding on sovereign matters, dating from the creation of the Irish Republic. Cooperation in law enforcement is routine. DRI

has no objection to the principle that the U.S. Attorney can get access to the emails of a suspected criminal located outside the United States. But in doing so, the United States must respect Irish law by using the MLAT procedures that the U.S. and Irish governments established to balance their respective sovereign interests. The District Court erred by losing sight of this.

ARGUMENT

I. DATA PRIVACY IS AN ACKNOWLEDGED HUMAN RIGHT PROTECTED IN IRELAND UNDER IRISH LAW, BUT THOSE PROTECTIONS ARE DESIGNED NOT TO IMPEDE CRIMINAL INVESTIGATIONS

Microsoft Ireland Operations Limited ("Microsoft-Ireland") is a wholly owned subsidiary of Microsoft Corporation and is a company registered in Ireland.[3] The datacenter hosting the email account is occupied and operated by Microsoft-Ireland.[4] The email data is not stored in the United States.[5]

Based on these facts, which are not disputed, no matter how the scope of U.S. jurisdiction is understood, it cannot be doubted that Ireland has jurisdiction over the data located in its territory and has a legitimate interest in how that data is handled.

---

[3] See Appendix ("A") at (A36).
[4] See (A37, A40.)
[5] See (A37, A40.)

A. Data Privacy Is A Significant Human Right

Under the Treaty on European Union ("TEU"),[6] the provisions and case law of the [European] Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR")[7] as developed by the European Court of Human Rights,[8] are general principles of EU law. Further, the EU recognizes the rights, freedoms, and principles set out in the Charter of Fundamental Rights of the European Union ("Charter").[9] Under Articles 7 and 8 of the Charter, EU residents are granted rights to the protection of data.[10]

ECHR Article 8(1) provides that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) states that there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and as necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or

---

[6] Consolidated Version of the Treaty on European Union, art. 6(3), May 9, 2008, 2008 O.J. (C 115) 15.
[7] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol Numbers 11 and 14, June 1, 2010, C.E.T.S. No. 005.
[8] TEU, art. 6(3).
[9] Charter of Fundamental Rights of the European Union, arts. 7-8, Mar. 30, 2010, 2010 O.J. (C 83) 389.
[10] Under Article 6(1) of the TEU, the Charter has equal status to the Treaties; accordingly the provisions of the Charter are binding in the interpretation of European law.

morals, or for the protection of the rights and freedoms of others.[11] The European Court of Human Rights ("ECtHR") has made clear that Article 8 applies to data stored by companies. In Wieser v Austria,[12] the ECtHR, finding a breach of ECHR Article 8, stated:

> The Court considers that the search and seizure of electronic data constituted an interference with the applicants' right to respect for their "correspondence" within the meaning of Art. 8. Having regard to . . . case law extending the notion of "home" to a company's business premises, the Court sees no reason to distinguish between the first applicant, who is a natural person, and the second applicant, which is a legal person, as regards the notion of "correspondence". It does not consider it necessary to examine whether there was also an interference with the applicants' "private life".

Ireland is a party to the ECHR and thus is bound to extend its protections to individuals within its jurisdiction.

The level of European public concern over the handling of personal data led to, in 1995, the adoption of an EU directive on data protection. A directive is an instruction to all EU Member States compelling them to enact legislation carrying-out the mandate of the directive.[13] This directive reconciled differing national traditions into a framework that provided a high level of protection for personal data.

---

[11] Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol Numbers 11 and 14, June 1, 2010, C.E.T.S. No. 005, at 4-5.
[12] Wieser v. Austria, 46 Eur. H.R. Rep. 54 (2008).
[13] Treaty on the Functioning of the European Union, art. 288, Oct. 26, 2012, 2012 O.J. (C 326) 47, 172.

Data protection and data privacy in Ireland follows EU rules set forth in Directive 95/46/EC ("the Data Protection Directive")[14] and Directive 2002/58/EC ("the "ePrivacy Directive").[15] The ePrivacy Directive confirmed the high value placed on protection of personal data. Recital 21[16] of the ePrivacy Directive provides that,

> Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

Manifest in the above passage is the very high importance attributed to protecting data against unauthorized disclosure. This goes beyond merely seeking to ensure that deliberate attempts to access such data are prohibited; any accessing of data not authorized by its owner is impermissible.

The importance of these principles was highlighted by the European Court of Justice ("ECJ"), at the instigation of *amicus* DRI. In Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources,[17] the ECJ

---

[14] Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).
[15] Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).
[16] Id. at 39.
[17] Case C-293/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Natural Res., (Apr. 8, 2014), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=59680.

annulled Directive 2006/24/EC on data retention.[18] That Directive set out rules for the retention of data regarding the use of electronic communication for the purpose of its later use by law enforcement authorities.[19] The Directive covered not the actual content of communications, but data on the use of communications tools.[20] Thus, the Directive required the routine capturing and storage of data about, for example, the use of a smartphone (such as date and location), but not the content of data recorded on, or transmitted from that phone.

In striking down the Directive, the Court observed that the mere retention of this usage data, even if it were never accessed, interfered with the fundamental right to privacy enshrined in the European Charter of Fundamental Rights. Indeed, establishing rules governing the access to stored data was itself an interference with the right to privacy. Highlighting the importance of protecting personal data under EU law, the Court, at paragraph 37 stated:

> [T]he interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out . . . wide-ranging, and it must be considered to be particularly serious. . . . [T]he fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

---

[18] Parliament and Council Directive 2006/24, 2006 O.J. (L 105) 54 (EC).
[19] Id. at 56.
[20] Id.

Where, as here, the data at issue is the actual content of an email account, rather than just time and location data, the sensitivity would be even higher.

In addition, Article 25[21] of the Data Protection Directive prohibits the transfer of personal data to countries outside the EU, unless those countries ensure an "adequate level of protection." This provision recognizes that individuals in the EU have an expectation that their personal data will be handled with, at a minimum, the degree of protection set out in the European legal framework. Surprising though it may seem, the transfer of data to a third country such as the United States is prohibited unless the U.S. recipient has in place rules which accord the data an equivalent level of protection to that prevailing under the Directive.

Notwithstanding these principles, European law also accepts the relevance of electronic data and data retention to criminal investigations, and in particular the fight against serious crime and terrorism. Interference with fundamental rights may be justified insofar as it is strictly necessary to achieve that objective: European law does *not* block the disclosure of information to foreign law enforcement authorities so long as there are sufficient protections of individual rights within the mechanism for such disclosure.

---

[21] Data Protection Directive, supra note 14, at 45.

B. European And Irish Law Provide Access For Law Enforcement Bodies To Personal Data

Under the Irish Data Protection Act 1988 (the "Act"), the owner of the account is the primary "data controller" in respect of the information it holds in Ireland.[22] Microsoft-Ireland is a "data processor"[23] and is limited in what it may do with account data. It may not export the data without complying with provisions of Irish law designed to preserve the privacy and integrity of the data.[24] But under Article 2 of the EU Data Protection Directive, the protections do not apply to data processed in the course of "the activities of the State in areas of criminal law."[25] Article 1(3) of the ePrivacy Directive contains an identical provision.[26]

Thus, European data protection legislation cannot be used to impede the effective investigation of criminal investigations. Irish law recognizes this in Section 8(b) of the Act, which provides that restrictions on disclosure of personal

---

[22] Data Protection Act 1988 § 1 (Act No. 25/1988) (Ir.), available at http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html, as amended by Data Protection (Amendment) Act 2003 (Act No. 6/2003) (Ir.) available at http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html (in section 1, setting out the definitions of data controller and data subject). The Act implemented the EU directives on data protection. See generally Article 29 Working Group Opinion 1/2010, p. 11, on the concepts of "Controller" and "Processor," available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (hereinafter "Working Group Opinion").

[23] See id.

[24] Working Group Opinion, supra note 22, at 5.

[25] Data Protection Directive, supra note 14, at 38.

[26] ePrivacy Directive, supra note 15, at 43.

data (such as the contents of an email account) do not apply if disclosure is required for the purpose of "preventing, detecting or investigating offences."[27]

II. SELF-EXECUTING MLAT PROCEDURES WERE SPECIFICALLY NEGOTIATED TO BALANCE U.S. INTERESTS IN EFFECTIVE LAW ENFORCEMENT WITH EUROPEAN AND IRISH INTERESTS IN DATA PROTECTION

Prior to 2006, the United States had entered into MLATs with fifteen EU nations, including Ireland. But in 2006, the United States put forward a comprehensive overhaul of those MLATs so as to allow the simultaneous implementation of modified MLATs with *twenty-five* EU Member States.[28] This was a milestone event, marking the first law enforcement agreement between the United States and the EU, and also allowed the United States and EU to complete a comprehensive extradition agreement with the EU. Mutual Legal Assistance Agreement with the European Union, S. TREATY DOC. NO. 109-13, Executive Summary at v (2006) ("MLAT Senate File").[29]

In urging ratification of the EU MLAT, President Bush hailed the agreement as an important development in the war against terror. Id. at v. Significantly, the

---

[27] Act, supra note 22, § 8(b).

[28] See U.S.-European Union Agreement on Mutual Legal Assistance, done Jun. 23, 2003, T.I.A.S. No. 10-201.1 (2003), which implemented the U.S.-Ireland Treaty on Mutual Legal Assistance, done Jan. 18, 2001, T.I.A.S. No. 13137 (2001).

[29] The Irish MLAT was signed prior to 2006, but had not entered into force as of then. Ireland ratified that MLAT contemporaneously with the entry into force of the EU MLAT. Id. at xxvi.

Administration said that one "innovation" of the EU MLAT was that it "establishes a comprehensive and uniform framework for limitations on the use of personal and other data." Id. at vi. Thus, by allowing "uniform improvements and expansions in coverage across much of Europe," the EU MLAT "will enable the strengthening of an emerging institutional relationship on law enforcement matters between the United States and the European Union, during a period when the EU is actively harmonizing national criminal law procedures and methods of international cooperation." Id. With respect to this case, there are three important aspects to the EU MLAT ratification.

First, the United States expressly recognized the important territorial interests of EU nations in information located within their borders. Thus, the United States said that "[m]utual legal assistance treaties generally address the production of records located in the requested State." MLAT Senate File at ix.

Second, the United States highlighted the specific data protection provisions enacted in the EU MLAT. Article 9 of the EU MLAT (which repeals Article 7 of the earlier Irish MLAT)[30] provides for limitations for the protection of personal data and replaced a use limitation provision used in prior MLATs.[31] Specifically,

[30] Id. at xxvii.
[31] Id. at xiv.

EU MLAT Article 9 was designed *to reconcile* the differences between US and EU data privacy laws.[32] As explained by the United States:

> Article 9(1) permits the requesting State to use evidence or information it has obtained from the requested State for its criminal investigations and proceedings [and] for preventing an immediate and serious threat to public security.[33]

Article 9(2)(a) then specifies that Article 9(1) does not preclude the requested State from imposing additional conditions, but Article 9(2)(b) makes clear that "generic restrictions with respect to the legal standard in the requesting State for processing personal data may *not* be imposed by the requested State as a condition under paragraph 2(a) to providing evidence or information."[34] This provision was so important that the parties included an Explanatory Note to the EU MLAT to drive home the importance of the MLAT procedures set out in Article 9(2)(b).

The Explanatory Note to the Treaty clarifies Article 9 by stressing that these MLAT procedures have been specifically designed to allow for a balancing of the competing sovereign interests inherent in cases like this one, and that generally MLAT procedures tilt *in favor* of data being provided:

> Article 9(2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand,

---

[32] Id. at xv.
[33] Id.
[34] Id. at xv (emphasis added).

> privacy interests), furnishing the specific data sought by the requesting State would raise difficulties so fundamental as to be considered by the requested State to fall within the essential interests grounds for refusal. A broad, categorical, or systematic application of data protection principles by the requested State to refuse cooperation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy of data (such as that the requesting State does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting State uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), may as such not be imposed as additional conditions under Article 9(2a).[35]

Thus, the United States made clear that the procedures in the EU MLAT not only were acceptable to it, but that these procedures were the way the United States and Europe had decided to balance their respective sovereign interests in the handling of personal and private electronic data.

Third, having created these MLAT procedures, the United States took an unusual step with regard to U.S. treaties. The United States informed Congress that both the EU MLAT "and [the 25] bilateral instruments" (e.g., including the Irish MLAT) "are regarded as self-executing treaties under U.S. law, and thus will not require implementing legislation for the United States." MLAT Senate File at vii. As amplified in the Senate Report on the EU MLAT, the treaty "will be implemented by the United States in conjunction with applicable federal

[35] EU MLAT, supra note 28, Explanatory Note (emphasis added).

statutes."[36] Thus, the EU and Irish MLATs of 2008 (when the U.S. Senate ratified the EU MLAT) were designed to be effective as is, and were designed to affect existing U.S. laws with no additional acts of Congress needed to bind the United States to the MLAT procedures created by these treaties.[37]

The record in this case also shows that the Irish MLAT does in fact work as intended. The former Attorney General of Ireland, Mr. Michael McDowell, was in office when the Irish and EU MLATs were negotiated, and has testified that these treaties were intended "to serve as the means for law enforcement authorities in the respective countries to obtain evidence located in the other treaty party." (A114.) McDowell also confirmed that "Ireland rarely refuses requests for information

---

[36] Mutual Legal Assistance Treaties with the European Union, Sept. 11, 2008, S. EXEC. DOC. NO. 110-13, 10 (2009) ("EU MLAT Senate Report"). Indeed, the self-executing status of these MLATs as a group was not affected by their having different terms and provisions for accomplishing the same goals. See MLAT Senate File at xvii-xix. In short, there were no "magic words" that conditioned the self-executing status of one nation's MLAT over another. Rather, the Senate recognized that "[i]n the absence of an applicable international agreement, the customary method for obtaining evidence or testimony in another country . . . tends to be an unreliable and time-consuming process" and that "the scope of foreign judicial assistance might also be limited by domestic information-sharing laws, such as bank and business secrecy laws." However, these treaties were "generally designed to overcome these problems." EU MLAT Senate Report at 2-3.

[37] As explained below, self-executing treaties are the exception rather than the rule, and create obligations enforceable under federal law. Self-executing treaties must be harmonized with existing federal law and given the fullest possible effect. See Whitney v. Robertson, 124 U.S. 190, 194 (1888); Blanco v. United States, 775 F.2d 53, 61-62 (2d Cir. 1985), discussed infra at 22.

made under the treaties" and that "the current MLAT procedures for fulfilling these requests are efficient and well-functioning." (A116.)[38]

In response, the United States has offered no evidence that the MLAT is any way slow, inconvenient, or otherwise inefficient. Instead, the United States simply has taken the position that it may circumvent the MLATs at will, that is, the self-executing Irish and EU MLATs do not need to be used as to evidence located outside the United States if the United States does not choose to use them.

III. THE DISTRICT COURT ERRED BY IGNORING THE SELF-EXECUTING EFFECTS OF MLAT TREATIES ENACTED AFTER THE STATUTE IN ISSUE

The Stored Communications Act, passed as part of the Electronic Communications Privacy Act of 1986 (the "ECPA"), 18 U.S.C. §§ 2701-2712, was enacted prior to 2008-09, when the EU MLAT was ratified and the Irish MLAT, as modified, became effective.[39] Thus, there is no doubt that the MLATs are later in time.

---

[38] Data on MLAT usage demonstrates that the MLAT regime is an often utilized tool in cross-border criminal investigation. For example, the United Kingdom Serious Fraud Office recorded 317 requests for assistance under the various MLATs concluded by the United Kingdom in the period from 2004 to 2011. See "Response from the United Kingdom Serious Fraud Office dated 14 June 2011 to Freedom of Information request on Mutual Legal Assistance figures," available at http://www.sfo.gov.uk/media/198535/mutual_legal_assistance_figures.pdf.

[39] The statutes were enacted in 1986, and have not been amended in any way since then that relates to information outside the United States.

It also is a fundamental principle of international law that each sovereign state is equal and entitled to prescribe laws and to adjudicate claims regarding persons or things within its sovereign territory.[40] Thus, there is no dispute that Ireland has jurisdiction to prescribe as to data stored within its borders, and that data privacy and data protection are longstanding, significant and seriously protected human rights in Ireland and the EU. To address the issues of competing jurisdiction that often arise when one nation seeks to investigate persons or things located beyond its borders, nations negotiate treaties to ensure that jurisdictional battles will not frustrate law enforcement *or* important human rights and public policies recognized by those states.

Here, the United States and EU did precisely that, and *acknowledged* in the Explanatory Note to the EU MLAT that these specific MLAT procedures were *designed* to balance law enforcement and data privacy issues *through the auspices of the treaty*. That intent must be given effect—and, in particular, this Court must interpret the MLATs so as not to render any of their terms a nullity. Factor v. Laubenheimer, 290 U.S. 276, 303-04 (1933) (words of a treaty should be liberally construed so as to not render any terms meaningless or inoperative) (citation

[40] See The Antelope, 23 U.S. (10 Wheat.) 66, 122 (1825) ("No principle of general law is more universally acknowledged, than the perfect equality of nations. Russia and Geneva have equal rights. It results from this equality that no one can rightfully impose a rule on another.").

omitted); Nielsen v. Johnson, 279 U.S. 47, 51 (1929) ("Treaties are to be liberally construed so as to effect the apparent intention of the parties.") (citation omitted).

The United States also took the extra and unusual step of designating the EU and Irish MLATs *self-executing*—a very rare designation for any U.S. treaty. Indeed, there is a general presumption against treaties being self-executing. See Mora v. New York, 524 F.3d 183, 200-02 (2d Cir. 2008) (courts are cautious to recognize private rights within treaty provisions). Here, however, the Executive expressly denoted the EU MLAT *and* the 25 associated national MLATs (which included the Irish MLAT) as self-executing and the Senate noted this in its report supporting ratification. See supra at 18-19. These statements by the Executive and Legislative branches are controlling as to the self-executing nature of the MLATs. In re Erato, 2 F.3d 11, 15 (2d Cir. 1993).

As a self-executing treaty, the Irish MLAT has the force of binding federal law, and must be given full effect as such. As this Court noted in Blanco v. United States, 775 F.2d 53, 61 (2d Cir. 1985), the "classic enunciation" of the rule on self-executing treaties is from Whitney v. Robertson, 124 U.S. 190, 194 (1888), in which the Supreme Court stated that a self-executing treaty

> is placed [by the Constitution] on the same footing, and made of like obligation, with an act of legislation. Both are declared by that instrument to be the supreme law of the land, and no superior efficacy is given to either over the other. When the two relate to the same subject, the courts will always endeavor to construe them so as to give effect to both . . . .

This rule highlights the error of the District Court. Here, the MLAT is comprehensive as to the matters it addresses. As the legislative history relating to ratification shows, the purpose of the MLATs was to overcome, by sovereign agreement, jurisdictional limitations on law enforcement—when they arose as to 25 (and now 28) EU nations—with respect to data privacy and protection. By signing the MLATs, the United States recognized the principle that the exercise of its jurisdiction, even where it might otherwise claim it has extraterritorial reach, is to be governed by the MLAT. This is even more true where, as here, the self-executing treaty comes into existence *after* the statute in question, in which case, if there is any inconsistency, it would be the later in time treaty that would govern. Whitney, 124 U.S. at 194; Blanco, 775 F.2d at 61.

Here, however, the District Court and the United States have ignored two governing rules of treaty application. *First*, the United States has chosen to read the MLATs as not constituting federal law that must be given effect. This, however, is expressly contrary to the EU MLAT Senate Report, which stated that the MLATs would "be implemented by the United States in conjunction with applicable federal statutes." EU MLAT Senate Report at 10. Nothing about the U.S. position is *"in conjunction with"* existing law. The United States sees the MLATs as having nothing to do with its warrant power even though there is no

dispute that the exercise of this warrant invades the province of Irish law as expressly covered by the Irish MLAT treaty.

Second, the U.S. position reads the MLATs so narrowly as to render the EU and Irish MLATs superfluous. Rather, than striving to read the MLATs in conjunction with the ECPA—as the Senate said would be done—the United States reads the MLATs as having no impact on existing U.S. law. But this crabbed reading of the MLATs—which effectively reads them out of existence—is the opposite of what this Court has mandated. This Court has said that the lower courts are to "harmonize" self-executing treaties like the MLATs with overlapping federal statutes. Cheung v. United States, 213 F.3d 82, 95 (2d Cir. 2000). If a statute and the treaties cannot be harmonized, then here, the treaties, as later in time, would govern. Blanco, 775 F.2d at 61-62. But, the District Court made no effort to harmonize. To do so, it should have recognized that no matter what the jurisdictional reach of the ECPA, because (i) the data sought was in Ireland and subject to Irish law, (ii) there is an Irish MLAT, and (iii) that MLAT was designated by the United States as self-executing, the MLAT conditioned how the United States could obtain this particular data.

Self-executing treaties create obligations. But, by compelling Microsoft to produce protected data from Ireland via an ECPA warrant, the District Court allowed the EU and Irish MLATs to be disregarded—i.e., treated as non-

obligatory. The U.S. position that the MLATs are somehow not mandatory is precisely contrary to the concept of an obligation and so effectively renders the EU and Irish MLATs a nullity. Adopting the U.S. position would allow the U.S. government unilaterally to substitute U.S. court compulsion for the balancing process represented by the MLAT information request procedures—and would destroy any incentive for any prosecutor to ever use the MLATs. This destroys the self-executing nature of the MLATs by effectively holding that absent some further act of Congress to require their use—which the United States represented was not necessary—the MLAT procedures do not have to be used. This is contrary to law and precedent and should be reversed.

CONCLUSION

For the foregoing reasons, *Amici Curiae* Digital Rights Ireland, Liberty, and the Open Rights Group urge the Court to reverse the District Court's decision, and order the United States to proceed under the U.S.-Ireland Mutual Legal Assistance Treaty.

Dated: December 15, 2014

By: /s/ *Owen C. Pell*

Owen C. Pell
Ian S. Forrester, Q.C.
Paige C. Spencer
WHITE & CASE
1155 Avenue of the Americas
New York, New York 10036
212-819-8891

Edward McGarr
Simon McGarr
Dervila McGirr
McGarr Solicitors
12 City Gate
Lr. Bridge St.
Dublin 8, Ireland

Counsel for Amici Curiae Digital Rights Ireland, Limited, Liberty, and the Open Rights Group

Certification of Compliance with Type-Volume Limitation, Typeface Requirements and Type Style Requirements

1. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(7)(B) because it contains 6,452 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionately-spaced typeface using Microsoft Word, 14 point font size.

Dated: December 15, 2014

WHITE & CASE LLP

By: /s/ Owen C. Pell

Owen C. Pell
Ian S. Forrester, Q.C.
Paige C. Spencer
1155 Avenue of the Americas
New York, New York 10036
Telephone: (212) 819-8891
Facsimile: (212) 354-8113

Counsel for Amici Curiae Digital Rights Ireland, Limited National Council for Civil Liberties and The Open Rights Group

Certificate of Service

I hereby certify that on this 15th day of December 2014, a true and correct copy of the foregoing Brief was served on all counsel of record via ECF pursuant to Local Rule 25.1(h).

Dated: December 15, 2014

WHITE & CASE LLP

By: /s/ Owen C. Pell

Owen C. Pell
Ian S. Forrester, Q.C.
Paige C. Spencer
1155 Avenue of the Americas
New York, New York 10036
Telephone: (212) 819-8200
Facsimile: (212) 354-8113

Counsel for Amici Curiae
Digital Rights Ireland, Limited
National Council for Civil Liberties and
The Open Rights Group