Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Access to extraterritorial evidence: The Microsoft cloud case and beyond

Dan Svantesson [a,*,1], Felicity Gerry, QC [b,**,1]

[a] Centre for Commercial Law, Faculty of Law, Bond University, Australia
[b] School of Law, Charles Darwin University, Darwin, Australia

Keywords:
Mutual Legal Assistance
Data privacy
Law enforcement
Investigative jurisdiction
Extraterritoriality
Human rights
Jurisdiction

ABSTRACT

A case involving Microsoft that is currently before the US courts has raised important issues between the respective legal regimes in the European Union and the United States, particularly in relation to the protection of personal data. The case in question has given rise to a degree of legal uncertainty and the outcome could have potentially serious implications for data protection in the EU. By seeking direct access to data held in the EU through the US judicial system, existing legal mechanisms for mutual assistance between jurisdictions may be being effectively bypassed. There are fundamental issues at stake here as regards the protection of personal data that is held within the European Union. This is clearly an area where technological advances have taken place in a very rapid fashion. The right to privacy should be afforded maximum protection whilst ensuring that law enforcement agencies have the necessary mechanisms at their disposal to effectively fight serious crime.[2]

1. Introduction

Anyone reading the technology section of any major newspaper could hardly have failed to notice the ongoing controversy between Microsoft, the US Government and the European Union. The US wants to force Microsoft to provide third-party content held on a server in Ireland. The EU says that Microsoft cannot transfer the relevant data to the US without considering EU data privacy law. Microsoft has become the proverbial 'meat in the sandwich'.

The case has raised fundamental issues on jurisdiction and extraterritorial evidence collection. The focus of many has been on the conflict between EU and US laws or legal procedure in the context of privacy or data protection but in fact the issues highlight a global problem: Where the activity of an individual or entity is across more than one State and Territory, whether that activity is criminal or commercial or some other form of behaviour, particularly where that activity is conducted online, the current legal responses are slow and ineffective. At the same time the ad hoc responses by some nations, notably the US, is intrusive and often lacking any solid foundation in international law.

* Corresponding author. Centre for Commercial Law, Faculty of Law, Bond University, Gold Coast, Queensland, 4229 Australia.
** Corresponding author. School of Law, Law Education Business & Arts, Charles Darwin University, Darwin, Northern Territory, 0909 Australia.
E-mail addresses: dasvante@bond.edu.au (D. Svantesson), Felicity.Gerry@cdu.edu.au (F. Gerry).

[1] Both authors contributed equally to the article.

[2] Dara Murphy T.D., Minister for European Affairs and Data Protection Minister for European Affairs and Data Protection requests legal brief by European Commission in Microsoft case http://merrionstreet.ie/en/News-Room/Releases/Minister_for_European_Affairs_and_Data_Protection_requests_legal_brief_by_European_Commission_in_Microsoft_case.html#sthash.s72C3wa3.dpuf.

http://dx.doi.org/10.1016/j.clsr.2015.05.007

Below, we will analyse the Microsoft cloud controversy. However, the issues associated with access to extraterritorial evidence go further than what surfaces in the Microsoft cloud case. To paint a slight more complete picture of the difficulties facing transnational litigants and investigators in this field, we also bring attention to and discuss issues arising not just in relation to internet intermediaries but particularly those involved in combatting transnational organised crime. Here the issue is not so much the proper law for the conduct of litigation but the collection of relevant evidence across territorial borders. This can arise in any international commercial action that requires evidential collection. In the cyber context this is where there is an intersection between criminal and commercial legal principles, particularly where breaches of privacy rules in some countries come with criminal penalties and/or significant financial sanction.

Take for example a legitimate international investment company operating across the globe using domain names and websites and call centres as well as banking institutions and then think about at least one case within the authors' experience[3] where an international investment fraud was carried out by use of falsified websites posted globally where the offenders duped investors into transferring funds, maintained the deception with falsified monthly reports and dissipated the assets before discovery where the actors were based in Asia but victims were global. The litigation that arises in the investigation of such an operation is both commercial and criminal and the evidence has the potential to be on servers in numerous locations. Decisions have to be made on which country has the jurisdiction to prosecute, where to serve warrants for the production of material and how to collate the material required not just to decide whether the operation is legitimate or not but to enable legal intervention at all. Often the result is piecemeal proceedings against identifiable individuals (sometimes themselves being exploited) and the main operators avoid sanction. If these issues are not addressed, and addressed globally there is little prospect of a solution.

Conversely, imagine an individual who is the subject of inappropriate litigation by a former business partner who seeks disclosure of trade information that will fundamentally compromise the business. The company is based in one country, the server in another and the litigious adversary in a third. Why should one person have easy access to private information of another – whether business or personal and how much more frightening is it the potential for Governments engaged in enquiries (commercial or criminal) could, through individual judges without legal precedent, bypass scrutiny and engage in draconian seizure policies.

In all of the above examples there is always evidence online (social media, emails, websites, messaging etc) and other more physical evidence within territories (confessions, diaries, accounts, company documents etc). How is it to be collected and used within a reasonable space of time? What of the data and privacy issues? All too often there is a knee jerk reaction to organised crime which inhibits the freedoms of law abiding people and is used as a foundation for intrusive State surveillance.

In the absence of a comprehensive global instrument in this sphere, we will consider the potential solutions in a cyber-context and will outline and discuss a number of different components that we suggest ought to be considered in any ethical and principled move towards improving international law and cooperation in the context of transnational extraterritorial evidence.

2. The Microsoft cloud case

In December 2013, the U.S. Government served a search warrant on Microsoft under the Electronic Communications Privacy Act of 1986 ("ECPA"). The warrant, issued by the United States District Court for the Southern District of New York, authorised the search and seizure of information associated with a specified web-based e-mail account that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"). Microsoft has opposed the warrant since the relevant emails are located exclusively on servers in Dublin, Ireland. Following a brief judgement where the District Court upheld the Magistrate's judgment, the matter is now to be decided in the Court of Appeal for the Second Circuit New York.

Microsoft filed its brief on 8th of December and interestingly it was followed by no less than 12 amicus briefs ('friend of the court' briefs) supporting Microsoft. The amicus briefs are even more interesting when one considers their diversity; they were filed by, for example (1) businesses such as Apple, Amazon, AT&T, Verizon and a range of media organisations, (2) academic experts including an expert on international law and a group of computer scientists (3) public interest organisations such as the Center for Democracy & Technology and the Digital Rights Ireland Limited, (4) the Irish Government and (5) a Member of the European Parliament. Such a united front amongst such a diverse group is rare but perhaps reflects the serious issues being discussed. What has followed is a great deal of high level international political attention. Here, we will briefly analyse the key legal issues involved in the case. However, to prepare ground for that discussion, we will first discuss jurisdiction in more general terms.

2.1. *Jurisdiction generally*

At Common law, questions of jurisdiction have traditionally arisen in the context of territorial borders. In *Ward v The Queen*[4] it was said that the accused was standing on the Victorian bank of the Murray River when he shot and killed the victim who as on the opposite bank in New South Wales. The High Court was faced with a federal system where each state had an obligation to not interfere with the affairs of other states and was asked to decide whether the act of murder had occurred at the point the trigger was pulled in Victoria or

[3] Various defendants prosecuted separately http://www.derbytelegraph.co.uk/Crook-4-5-million-scam-ordered-pay-66-000/story-15727504-detail/story.html and http://www.bbc.com/news/uk-england-derbyshire-24281949 and http://www.walesonline.co.uk/news/local-news/felinheli-woman-jailed-document-frauds-2056080.

[4] (1980) 142 CLR 308.

where it entered the deceased in New South Wales. The case was in fact resolved by historical evidence which demonstrated that the borders had been incorrectly identified and the defendant had been wrongly tried in Victoria.

This follows the common law tradition that if an act takes place within the relevant country, the courts of that country will have jurisdiction to try the offence subject to the allocation of business between court centres and the selection of the appropriate court. In 1891, Lord Halsbury LC stated: "All crime is local. The jurisdiction over the crime belongs to the country where the crime is committed …".[5] Only124 years later this is clearly an impossible approach.

Outside of the common law tradition, jurisdiction was to a great extent based on nationality; trying citizens for their conduct, although historically this was conduct within territorial boundaries in any event. More recently prosecutorial jurisdiction has been the subject of codification or statutory exception depending on the State concerned and the legal tradition. The general tendency is to enlarge jurisdiction to prosecute beyond territorial boundaries but these are piecemeal and generally related to conspiracies or child abuse. Such extraterritorial jurisdiction is often dealt with in commercial litigation by lengthy arguments on proper law. It is here that the law is confronted by increasing technology and transport that cuts across borders with great ease. Countries now have competing claims to jurisdiction and issues of Parliamentary Sovereignty can makes commercial cases inherently political.

Decisions on jurisdiction can also be evidential on the grounds of nexus – particularly in conspiracies – this can include factors such as the location of witnesses and other evidence and in the context of extradition can include consideration of whether an alleged offence is also an offence in the requesting country. The Swedish extradition request for Julian Assange led the English courts into protracted consideration of whether the laws of Sweden and England on rape were sufficiently similar to allow for extradition.[6] Sometimes there are also issues of fairness and if a legal team in one country asserts that an individual cannot receive a fair trial in another, this is also intensely political. It is not hard to see why; in the context of commercial litigation the Microsoft case has created such a significant reaction.

In the criminal law context, where there is a significant degree of mutual co-operation between agencies, the competent authority will be the one where there is a clear link between the actions of the domestic police and the proceedings to which the defendant becomes subject during the course of the investigation.[7] Many States have enacted legislation to allow for extraterritorial jurisdiction to prosecute criminal offending that has a nexus with the prosecuting State or is committed by a citizen of that State in another. The effectiveness of such legal proceedings depend on mutual legal assistance treaties (MLAT) where there is agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws. These have been developed over time, rarely apply to commercial litigation and are slow to react to technological development.

It is immediately apparent that jurisdiction can be separated into more than one legal issue. For example, it is customary to distinguish between three different forms of jurisdiction; that is: (1) prescriptive (or legislative) jurisdiction, (2) judicial (or adjudicative) jurisdiction, and (3) enforcement jurisdiction. However, not least due to the increase in cross-border contacts that stem from the Internet, it is useful to also consider a fourth type of jurisdiction – what we can call investigative jurisdiction.[8]

As is well known, prescriptive (or legislative) jurisdiction relates to the power to make law in relation to a specific subject matter. Judicial (or adjudicative) jurisdiction, as the name suggests, deals with the power to adjudicate a particular matter. And, finally, enforcement jurisdiction relates to the power to enforce the law put in place, in the sense of, for example, arresting, prosecuting and/or punishing an individual under that law.

Investigative jurisdiction – where considered at all – is treated as a component of enforcement jurisdiction under conventional thinking.

Investigative jurisdiction relates to the power to investigate a matter and must be kept separate from the jurisdiction to make rules, adjudicate disputes and to actually enforce the law.

Perhaps the most important reason for treating investigative jurisdiction as a separate and distinct form of jurisdiction is found in the fact that, a state may have a range of reasons for wanting to investigate a matter without ending up exercising adjudicative jurisdiction over the matter, or applying prescriptive jurisdiction to the matter, or indeed, seeking to take any enforcement actions against the person it investigates. Such an outcome would, for example, be the case where (1) the investigation shows that there is no reason to pursue the matter, or more importantly (2) where the investigation shows that the matter is best dealt with by a request seeking another state to claim adjudicative, legislative and enforcement jurisdiction over the matter. In light of this, it does not make sense to bundle investigative jurisdiction with enforcement jurisdiction, as is traditionally done.

The instances where investigative jurisdiction plays a central role are numerous, for example, in the context of data privacy law and in areas such as consumer protection – areas where complaints often are best pursued by bodies such as privacy commissioners/ombudsmen and consumer protection agencies. Indeed, the crucial importance of distinguishing investigative jurisdiction from other forms of jurisdiction was at the core of a 2007 decision by the Federal Court of Canada.

In *Lawson v Accusearch Inc dba Abika.com* [2007] 4 FCR 314, the Privacy Commissioner of Canada was forced to defend, in court, her decision to decline to investigate a complaint made by Lawson of the *Canadian Internet Policy and Public Interest Clinic* against a US-based corporation. Harrington J of the Federal Court stated that:

[5] *Macleod v. Attorney-General (NSW)* [1891] AC 455 at 458.

[6] *Assange v Sweden* [2012] UKSC 22, 2011] EWHC 2849 (Admin).

[7] See for example *George Francis Burns v HM Advocate* [2008] UKPC 63, a prosecution relating to indecent images of children.

[8] The discussion of "investigative jurisdiction" draws, and expands, upon: Dan Svantesson, Extraterritoriality in Data Privacy Law (Ex Tuto Publishing, 2013), at 67–69.

> *I agree with her [the Privacy Commissioner of Canada] that PIPEDA [Personal Information Protection and Electronic Documents Act] gives no indication that Parliament intended to legislate extraterritorially. […] [However, the] Commissioner does not lose her power to investigate because she can neither subpoena the organization nor enter its premises in Wyoming. […] It would be most regrettable indeed if Parliament gave the Commissioner jurisdiction to investigate foreigners who have Canadian sources of information only if those organizations voluntarily name names. Furthermore, even if an order against a non-resident might be ineffective, the Commissioner could target the Canadian sources of information.*
>
> *I conclude as a matter of statutory interpretation that the Commissioner had jurisdiction to investigate, and that such an investigation was not contingent upon Parliament having legislated extraterritorially[.]*[9]

The currently ongoing dispute between Microsoft and the U.S. Government about the Government's attempt to make Microsoft provide details of an e-mail account held by Microsoft's subsidiary in Ireland is a good illustration of why the time is right to distinguish, define and delineate investigative jurisdiction.

Looking at the *Microsoft* case, the very fact that dispute arose in the first place highlights that contemporary jurisdictional thinking has failed to adequately address the challenges posed by the Internet in general, and perhaps cloud computing in particular. This failure may party be blamed on the law's unwillingness to part with traditional categorisations and thinking so as to recognise models and structures that better correspond to the new technological reality.

Here we focus on evidence collection starting with the detail of the *Microsoft* case.

2.2. *Presumption against extraterritoriality*

There is a longstanding presumption in U.S. law that "[w]hen a statute gives no clear indication of an extraterritorial application, it has none."[10] This follows the common law tradition. In Lord Halsbury's language, it is a "local" law. Microsoft argues that "the search and seizure occur in Dublin, where the emails reside"[11] and thus is extraterritorial. Or, put differently, as summarised by the magistrate judge James C. Francis IV, Microsoft is arguing that:

> *Federal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States. Therefore, […] to the extent that the warrant here requires acquisition of information from Dublin, it is unauthorized and must be quashed.*[12]

Commenting on this assertion, the magistrate judge observed that: "That analysis, *while not inconsistent with the statutory language*, is undermined by the structure of the SCA [Stored Communications Act (passed as part of the ECPA)], by its legislative history, and by the practical consequences that would flow from adopting it."[13] (emphasis added).

This is a key sentence that perhaps can decide the matter. In light of the reasoning by the magistrate judge that Microsoft's analysis is *not inconsistent with the statutory language* it is hardly possible to say that the relevant law gives a *clear indication of an extraterritorial application*, and thus it has none. However, the conclusion was that extraterritorial jurisdiction could be implied. This was justified by reference to the fact that there is an equally strong tradition that the interpretation of a statute includes consideration of Parliament's intention. To avoid deviating too far from the theme of this article, we will not delve into that matter in detail here.

2.3. *Extraterritorial or not?*

The real question is consequently whether the issue of extraterritoriality arises in the first place. If it does, Microsoft must be successful, and if it does not, the inquiry will have to go on. Unsurprisingly, Microsoft says the issue of extraterritoriality obviously does arise, and the U.S. Government claims that it equally obviously does not. The difference in perspective is apparent throughout, but is particularly well illustrated in the following quote from the Government's brief of 9 June 2014:

> *Relying on Section 432(2) of the Restatement (Third) of Foreign Relations, Microsoft argues that '[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state.' […] But requiring the disclosure of records by a U.S. company does not involve any enforcement activity by government personnel on foreign territory, which is the concern of that section.*[14]

Reading this quote carefully, it is obvious that Microsoft and the U.S. Government are talking about two different things, and that they are arguably both correct. It is true, as the Government says that there is no *enforcement activity* on foreign territory. However, and this is important, there is an exercise of law *enforcement functions* in the territory of another state. In other words, the Government looks exclusively to the location from which jurisdiction is exercised (the US). Microsoft considers also the extraterritorial effects and they occur in Ireland. In this way, the US Government gives extraterritoriality a narrow definition, while Microsoft gives it a broader definition. It is in a sense just the same issue that arose in *Ward v The Queen* albeit a virtual shot and across an ocean rather than a river.[15]

---

[9] *Lawson v Accusearch Inc dba Abika.com* [2007] 4 FCR 314 https://www.canlii.org/en/ca/fct/doc/2007/2007fc125/2007fc125.html.

[10] *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247 (2010) at 255.

[11] Brief by Appellant Microsoft Corporation, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation (No. 14-2985-cv) at 26.

[12] In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., __ F. Supp. 2d. __, No. 13 Mag. 2814, 2014 WL 1661004, at *11 (S.D.N.Y. Apr. 25, 2014) 8–9.

[13] *Id.* at 9.

[14] Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation (1:13-mj-02814) at 21.

[15] Ibid paragraph 10.

In support of its approach, the Government states that: "The principle against extraterritoriality presumes that Congress does not intend for a law to *apply* extraterritorially. It does not presume Congress's intention to be that the law has no incidental effects outside the country whatsoever."[16] This, the Government supports by referring to the following quote: "Even where the significant effects of the regulated conduct are felt outside U.S. borders, the statute itself does not present a problem of extraterritoriality, so long as the conduct which Congress seeks to regulate occurs largely within the United States."[17]

However, here we are just going around in circles since the quote above may equally well support Microsoft's view depending on what we characterise as the *conduct* in question. In our view, we have (like Mr Ward's bullet) here hit a dead end.

2.4. *From proxy principles to core principles and more*

To understand which interpretation of extraterritoriality we should favour, it is necessary to view the presumption against extraterritoriality in its proper light. This presumption, just like the *Charming Betsy doctrine* also discussed in the context of the case[18] (put simply 'statutes should be construed to be consistent with international law') are proxies for, or expressions of, the one and same core principle; that is, the presumption that Congress does not wish to enact law that will create clashes of interest with foreign states. In other words the presumption against extraterritoriality is just a proxy principle conveniently adopted as the focal point in a world, at the time, dominated by a territorial focus. The question that arises here is whether, perhaps unwittingly, the Magistrate in the Microsoft case, exposed a modern approach to legislative interpretation based on community needs not individual sovereignty.

This in turn gives rise to examination of Parliamentary Sovereignty in the context of a global community. The court here was required to balance essential rights to a fair trial. Without the necessary evidence, held by an organisation that operates in more than one State, the litigation would be compromised. At the same time, the issues engaged rights to privacy. These are not merely questions for the US Constitution or the equivalent Irish instruments but for the international community. The Internet is global and so there is an argument that courts must take a global approach in deciding the operation of domestic legislation.

The tradition of strict dualism, from decisions such as *R v Secretary of State for the Home Department*; *Ex parte Bhajan Singh*[19] which expounded the classical divide has changed. Modern theoretical underpinning of dualist systems (national and international) recognize that courts can accommodate international law whether given effect by valid legislation or by assisting in the development of the common law. Even in cases where international law has not, by legislation or valid executive action, been incorporated into national law, there are occasional circumstances where that law may be used by judges and other independent decision-makers in the national legal system to influence their decisions. This is particularly so in the case of international human rights principles as they have been expounded, and developed, by international and regional bodies.

An expression of what The Hon Justice Michael Kirby AC CMG has called this "modern approach" was given in February 1988 in Bangalore, India, in the so-called *Bangalore Principles*. The meeting was chaired by Justice P N Bhagwati, a former Chief Justice of India. Present was Lord Lester of Herne Hill. Relevantly, the *Bangalore Principles* state, in effect[20]:

- International law (whether human rights norms or otherwise) is not, in most common law countries, part of domestic law.
- Such law does not become part of domestic law until Parliament so enacts or the judges (as another source of law-making) declare the norms thereby established to be part of domestic law.
- The judges will not do so automatically, simply because the norm is part of international law or is mentioned in a treaty – even one ratified by their own State.
- But if an issue of uncertainty arises (by a gap in the common law or obscurity in its meaning or ambiguity in a relevant statute), a judge may seek guidance in the general principles of international law, as accepted by the community of nations.
- From this source material, the judge may ascertain and declare what the relevant rule of domestic law is. It is the action of the judge, incorporating the rule into domestic law, which makes it part of domestic law.

In terms, the *Bangalore Principles* declare:

- [T]here is a growing tendency for national courts to have regard to these international norms for the purpose of deciding cases where the domestic law – whether constitutional, statute or common law – is uncertain or incomplete *(Bangalore Principles* No 4)
- It is within the proper nature of the judicial process and well-established judicial functions for national courts to have regard to international obligations which a country undertakes – whether or not they have been incorporated into domestic law – for the purpose of removing ambiguity or uncertainty from national constitutions, legislation or common law (B*angalore Principles* No 4)

[16] Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation (1:13-mj-02814) at 19.

[17] *Envtl. Def. Fund.* v. *Massey*, 986 F.2d 528, 531–32 (D.C. Cir. 1993).

[18] See e.g.: Amicus brief of Verizon etc https://cdt.org/files/2014/12/14-2985-Amicus-brief-of-Verizon-Cisco-HP-eBay-Salesforce.com-and-Infor.pdf.

[19] [1976] 1 QB 198 at 207.

[20] Taken in part from Kirby, Michael – "Domestic Implementation of International Human Rights Norms" [1999] AUJlHRights 27; (1999) 5(2) Australian Journal of Human Rights 109.

Laws develop in line with international law, particularly in the context of Commonwealth land rights.[21] Here we have property rights in the context of the contents of a server. This is logical to ensure conformity where, for example, the law of one country has been opened up to international remedies to individuals pursuant to accession to international instruments such as the Optional Protocol to the International Covenant on Civil and Political Rights. This brings to bear on the common law the powerful influence of the Covenant and the international standards it imports. The law of an individual State may not necessarily conform to international law, but international law is a legitimate and important influence on the development of domestic interpretation, especially when international law declares the existence of universal human rights. A doctrine founded on unjust discrimination in the enjoyment of civil and political rights demands reconsideration. It is contrary both to international standards and to the fundamental values to entrench a discriminatory rule.[22]

It follows that international obligations *must* be considered in the performance of an administrative decision-making process. Effectively the interpretation of the US instrument requires due consideration of individual rights to a fair hearing as against the rights of privacy. This leaves the courts responsible for enforceable rights, utilising international law where an appropriate gap appears or where a statute is ambiguous or there is a conflict between legislation. Arguably the same issues would then necessarily apply should there be litigation in the context of any breach of EU legislation by complying with the terms of the warrant. The Microsoft case highlights not just the tasks of individual judges but also the need for legal systems to work cooperatively in general harmony with the development of the international law of human rights.

Whenever we are trying to apply the law to novel phenomena that need to become the subject of clear legal rules, we need to cut away the undergrowth of proxy principles and identify the core principles that are reflected in those proxy principles. Only then will we be able to focus on the considerations and values that truly are to be balanced.

Applying this to the matter at hand we can usefully ask whether jurisdictional claims with an extraterritorial effect can create clashes of interest with foreign states. Here we need not dig particularly deep; the answer is of course yes as is evidenced by the strong European reactions to the Microsoft case.[23]

U.S. Government may of course continue pushing its argument that there is no extraterritoriality in the case. However, we doubt that this senior court should have any problems disposing of such an outdated and overly simplistic claim about extraterritoriality.

Having reached this conclusion, the more interesting question is of course whether a sensible system could be developed allowing more effective law enforcement access to cloud content. We return to that topic further below.

3. The problems more broadly

The analysis of the Microsoft cloud case above has highlighted some aspects of the complexities associated with securing access to extraterritorial evidence, particularly in the cloud computing context. However, as we demonstrate below, there are several other complications that also must be taken into account.

3.1. *Domestic crime may require cross-border investigation*

The reality is that with increased globalisation comes an increased globalisation of criminal activities, and just like most people now communicate via email rather than postal mail, and store their data in the cloud rather than locally on their computers, tablets or phones, criminals also communicate via email rather than postal mail, and store their data in the cloud rather than locally on their computers, tablets or phones. The obvious question is to what extent we can allow this development to complicate law enforcement, and the concerns involved are well illustrated in the U.S. Government's Brief in Support of the Magistrate Judge's Decision:

> *In today's digital environment, email and other electronic communications are used extensively by criminals of all types in the United States and abroad, from fraudsters to hackers to drug dealers, in furtherance of violations of U.S. law. The ability to obtain electronically stored information from domestic service providers—pursuant to judicial authorization as required by the SCA—is a fundamental component of effective modern law enforcement. Yet such information, like the data sought by the Warrant here, can be maintained in any location and moved around the world easily, at any time and for any reason. Were Microsoft's position adopted, the Government's ability to obtain such information from a provider would turn entirely on whether it happens to be stored here or abroad, even though the provider, based in the United States, maintains control over the data wherever it is. Such a regime would be rife with potential for arbitrary outcomes and criminal abuse.*[24]

In other words, should criminals be able to complicate and prolong investigations by introducing an international dimension simply by storing data on a server in another country?

[21] See the remarks of Justice Brennan (with the concurrence of Chief Justice Mason and Justice McHugh) in *Mabo v Queensland \t(No 2)*. In the course of explaining why a discriminatory doctrine, such as that of *terra nullius* (which declined recognition of the rights and interests in land of the indigenous inhabitants of a settled colony such as Australia) could no longer be accepted as part of the common law of Australia, Justice Brennan said:

[22] See *Derbyshire County Council v Times Newspapers Ltd.*

[23] Allison Grande, *EU Official Slams US For Asking Microsoft For Overseas Data*, Law360.com (Jun. 30, 2014), http://www.law360.com/articles/553140/eu-official-slams-us-for-asking-microsoft-for-overseas-data.

[24] Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (1:13-mj-02814) at #.

In some cases, a lack of forward-thinking amongst law makers may limit law enforcement efforts beyond what arguably is necessary. Imagine, for example, that a law enforcement agency, backed by a warrant, seized a laptop computer belonging to a suspected criminal. Ten or fifteen years ago the situation would be relatively uncomplicated in that the data the law enforcement agency would be looking for would typically be stored on the laptop. But today, it is equally, or more, likely that the data is stored in the cloud. Thus, the question arises as to whether the warrant also gives access to the cloud data – data that may be equally easy to access as the data stored locally on the laptop.

This issue came into the limelight to some degree in Australia during the Legal and Constitutional Affairs Legislation Committee's Inquiry into the Intelligence Services Legislation Amendment Bill 2011. The proposal included a change of the wording of Paragraph 25(4)(a) of the Australian Security Intelligence Organisation Act 1979 (Cth) from "stored in the target computer", to "held in the target computer at any time while the warrant is in force". It was pointed out in one submission[25] that this change remains focused on data present on a particular computer, and thus does not cater for cloud computing situations like the one described above.

This prompted a Supplementary Submission by the Attorney-General's department in which it was stressed that:

> *The term data 'held' in the target computer is preferred as the more technologically neutral term. It would clearly encompass data that is stored on a more permanent basis, such as in a hard drive, as well as data that may be held in the computer on a temporary basis or from time to time, as is the intention of the provision. The amendment further clarifies this intent by providing that the Attorney-General may issue a computer access warrant 'for the purpose of obtaining access to data that is relevant to the security matters and is held in the target computer at any time while the warrant is in force'.*[26]

The problem is obvious; where cloud data is not downloaded to the target computer during the time of a valid warrant, it would seem that such data is beyond the warrant. This, perhaps more than any statement demonstrates how the law cannot keep up with technology unless there is a set of general principles that can be applied. In the same way as a murder can take place in a myriad of different ways, legislation must adapt to encompass principles of storage of material. It is here that the practical reality recognised by the Magistrate in the Microsoft case becomes all important: If a statute is to be interpreted in the modern global context it must be interpreted in the light of modern methods – Parliaments intention becomes – what did the legislature intend to do having regard to modern jurisprudence and modern communication – the alternative is endless qualifications which make legislation even more unworkable. This is not to say that the sensibilities of the State that is the subject of the warrant need to be offended but that the global community acts together in the context of evidence collection – balancing together rights and responsibilities. In our view, this can work but only with reasoned approaches and effective scrutiny.

3.2. *Human Rights*

We recognise that the prevalence of cybercrime is used as a justification for intrusive surveillance and over regulation.[27] Intrusive surveillance and over regulation threaten privacy right of individuals.[28] The major issue in the Microsoft case that has caused so much intervention is the risk that competing interests on an individual, corporate, government and global level will not be balanced. The same concerns arose in the Court of Justice of the European Union (CJEU) decision in the case of *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*[29] to require Google to enforce a so-called 'right to be forgotten' (more accurately, a 'right to delisting') which effectively makes Google responsible for Internet regulation, creating fears about control of the Internet.

Data privacy was obviously a key element in the Microsoft cloud case discussed here. While in that case we saw a clash between the European emphases on data privacy on the one hand, and U.S. calls for efficient law enforcement on the other hand, the reality is of course both more nuanced and more complex.

As has been pointed out elsewhere,[30] when discussing privacy in the context of cyber crime it is important to bear in mind that, privacy is typically negatively affected by both cyber crime, and attempts to address cybercrime. This dualism places regulators in a difficult position as their attempts to protect against, and investigate, cyber crime, may involve methods that are in themselves privacy invasive. Thus, regulators will often have to balance the protection of privacy with the need to effectively address cyber crime.

In performing such a balancing act, regulators must bear in mind that privacy is a fundamental human right. Perhaps most importantly, privacy is a recognised human right in the *International Covenant on Civil and Political Rights (ICCPR)*.

[25] Submission by Dr Dan Svantesson to the Legal and Constitutional Affairs Legislation Committee's Inquiry into the Intelligence Services Legislation Amendment Bill 2011, 26 May 2011, https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=3da24ca1-9864-4c55-8183-c17d01d48698.

[26] Supplementary submission by the Attorney-General's Department to the Legal and Constitutional Affairs Legislation Committee's Inquiry into the Intelligence Services Legislation Amendment Bill 2011, 26 May 2011, https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=b37cff07-ca19-4603-8ff9-ab9f50a3db2b at 5.

[27] Felicity Gerry QC and Nadya Berova, *The rule of law online: Treating data like the sale of goods: Lessons for the Internet from OECD and CISG and sacking Google as the regulator*, 30 CHAR. DAR. UNIV. COMP. L. & SEC. REV.469 (2014).

[28] *Race to the Bottom" Corporate Complicity in Chinese Internet Censorship*, HUMAN RIGHTS WATCH, 5 (Aug. 10, 2006), http://www.hrw.org/reports/2006/china0806/3.htm.

[29] Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González (Case C-131/12).

[30] Submission by the Australian Privacy Foundation In response to the House of Representatives Standing Committee on Communications' Cyber Crime Inquiry (6 August, 2009), https://www.privacy.org.au/Papers/Cybercrime-090805.doc.

Consequently, privacy protection is not optional – a regulator must take account of peoples' legitimate expectations of privacy in any attempt to regulate, and investigate, cyber crime.

In July 2012, the UN Human Rights Council adopted a resolution affirming the application of rights online, especially freedom of expression. This resolution confirmed that both Articles 19 of the *The Universal Declaration of Human Rights* (UDHR) and ICCPR are "applicable regardless of frontiers and through any media of one's choice"[31] and that any attempt by governments to illegitimately censor or block Internet content would be incompatible with those instruments.[32] More recently, on June 20, 2014, the Council called upon all states to address the protection of these common standards in laws that pertain to the Internet.[33] In the Microsoft case the court was concerned with the contents of a server. Whilst anonymity is part of the culture in relation to the Internet, here the consideration related to business communications. According to the UN Special Rapporteur, Frank La Rue communications should remain secure, i.e. "individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion." If individuals wish to be anonymous in their communication, this must be preserved so that individuals may "express themselves freely without fear of retribution or condemnation."[34] In a recent report by the Office of the UN High Commissioner for Human Rights, it is reiterated that any State "surveillance measures must not arbitrarily or unlawfully interfere with an individual's privacy, family, home or correspondence; Governments must take specific measures to ensure protection of the law against such interference".[35] The collection and retention of communications data amounts to an "interference … whether or not those data are subsequently consulted or used."[36]

The ICCPR provides for the freedom of expression in Article 19(2):

> *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds,* ***regardless of frontiers****, either orally, in writing or in print, in the form of art, or* ***through any other media*** *of his choice.*[37]

If we are considering global conventions and/or the balancing exercise that an individual judge has to engage in then it is important to remember that this right is a qualified right and can be restricted, per Article 19(3). The requirement of a limitation to be "provided by law" requires that the law should be "formulated with sufficient precision" to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public".[38] The law must also "provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not".[39] Any restriction must be proportionate to the protective aim and must be the least intrusive measure.[40] This principle of proportionality must also account for the form of the expression, including its means of dissemination.[41] Here it seems those requirements were not available and the Magistrate in the Microsoft case filled the gap.

4. Components of a solution

In the above, we have highlighted several serious issues facing law enforcement, prosecutors and private parties seeking to secure access to extraterritorial evidence, not least in the cloud computing context. There can be no doubt that much work is needed to address these issues, but equally, there can be no doubt that we *must* address these issues.

In the below, we discuss some mechanisms that are of relevance and that should be considered in future attempts at improving the operation of the law in this field.

4.1. *Mutual Legal Assistance Treaties*

Any search for solutions in this field must take as its point of departure the observation that there is already a system in place for law enforcement agencies accessing data in a foreign country like how the U.S. government wanted to access data held in Ireland. The previously mentioned MLAT regime is in place in relation to a number of countries, including Ireland:

> *Mutual Legal Assistance is an agreement, usually by treaty, between two or more countries to provide assistance to each other on criminal legal matters. The types of assistance that can be provided through MLA include: service of documents; search and seizure; restraint and confiscation of proceeds of crime; provision*

[31] U.N. Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, para. 1, A/HRC/20/L.13 (June 29, 2012).
[32] *Id.* at para. 15.
[33] U.N. Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, para. 5, A/HRC/26/L.24 (June 20, 2014) ("Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development".).
[34] *Id.* at para. 23.
[35] *Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age*, para. 15, A/HRC/27/37 (June 30, 2014) http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.
[36] *Id.* at para. 20; *See also, Weber and Saravia v. Germany*, App. No. 54934/00, Eur. Ct. H.R. para. 78 (2006); *Malone v. UK*, App. No. 8691/79, Eur. Ct. H.R. para. 64 (1984) (Both of these ECtHR cases indicate that even the mere possibility of communications information being captured creates an interference with the right to privacy).
[37] International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171. Article 19(2) (emphasis added).
[38] *General Comment No. 34, supra* note 23 at para. 25; *See also*, Communication No. 578/1994, de Groot v. The Netherlands, Views adopted on 14 July 1995.
[39] *General Comment No. 34, supra* note 23 at para. 25.
[40] *Id.* at para. 34.
[41] *Id.*

of telephone intercept material; and the facilitation of taking of evidence from witnesses. The agreements themselves, whilst indicating the points of contact in both countries, do not specify the end to-end process. This is governed by a mixture of national laws: laws covering international co-operation and laws relating what is being requested. The MLA process is therefore determined by a combination of domestic law and bilateral and multilateral treaties on international crime. MLA is resilient because it is the only process that ties together the laws of both receiving and requesting country, making it legally robust at all stages.[42] *(internal footnotes removed)*

In the Microsoft case, the parties present very different views of the efficiency of the MLAT system. Microsoft states that:

If the Government needs to obtain any private papers from Ireland [...] it relies on the MLAT or other bilateral arrangements to do so. [...] The MLATs create well-defined procedures to obtain the precise type of private emails at issue here. In fact, some of the processes are superior to the ones in place for physical evidence.[43]

In contrast, U.S. Government observes that:

Microsoft's rosy view of the efficacy of the MLAT process bears little resemblance to reality. [...] an MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the law enforcement resources it has to spare for outside requests for assistance, and the procedural idiosyncrasies of the country's legal system.[44]

Importantly, Microsoft's view gains support from the *amicus* brief filed by the Irish Government: "Ireland continues to facilitate cooperation with other states, including the United States, in the fight against crime and would be pleased to consider, as expeditiously as possible, a request under the treaty, should one be made".[45]

It is difficult to escape the conclusion that the U.S. Government's complaints about the MLAT process would have been more relevant to the case at hand had they been able to point to particular difficulties getting Irish cooperation under the MLAT system prior to seeking a domestic warrant.

Nevertheless, there is no doubt that the MLAT system needs a substantial overhaul. One leading commentator in this field – Gail Kent – has pointed to set of principles that can guide future work on the topic of MLATs:

We should be explicit about the principles underpinning international data sharing. From looking at work carried out by the separate stakeholder groups, these principles could be:

i. respect human rights, notably the right to privacy and freedom of expression as outlined in the United Nations International Covenant on Civil and Political Rights;
ii. focus on sharing data to support the investigation of serious crimes, organized crimes, terrorism and cyber-crime clearly impacting on the jurisdiction making the request. It should also support existing measures to prevent threats to life and harm to children;
iii. not support any intervention or activities of a political, military, religious or racial character. There must be integrity of motive, with no hidden agendas on the stated purpose of the investigation or the reasonable belief that an offense was committed;
iv. support requests for information that are proportionate and necessary to the investigation, including relating to specific accounts and specific investigations;
v. support requests that are lawfully authorized and where this authorization can be authenticated;
vi. provide simplicity and clarity: all stakeholders – service providers, users, government and law enforcement – deserve clear and simple rules;
vii. be transparent to all stakeholders, including internet users, internet service providers, governments, law enforcement, academics and non-governmental organizations;
viii. support joint working between government and the private sector nationally and internationally to effectively tackle crime;
ix. support effective global co-operation to tackle crime by providing an efficient and secure system;
x. have national and international governance and safeguarding structures, collectively determined by participants, that support the principles and ensure the long term success of the system [46]; (internal footnotes and some formatting removed)

In any case, it is not our aim here to analyse in depth the efficiency of the MLAT system. It is, however, important to remember that any alternative path one proposes will operate side-by-side with this existing established system; it will be complimenting the MLAT system.

[42] Kent, Gail, Sharing Investigation Specific Data with Law Enforcement - An International Approach (February 14, 2014). Stanford Public Law Working Paper. Available at SSRN: http://ssrn.com/abstract=2472413 or http://dx.doi.org/10.2139/ssrn.2472413, at 5.

[43] Brief by Appellant Microsoft Corporation, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (No. 14-2985-cv) at 57–58.

[44] Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (1:13-mj-02814) at 25–26.

[45] Amicus Curiae Brief in Support of Appellant Microsoft Corporation by Ireland, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (No. 14-2985-cv) at 8.

[46] Kent, Gail, Sharing Investigation Specific Data with Law Enforcement - An International Approach (February 14, 2014). Stanford Public Law Working Paper. Available at SSRN: http://ssrn.com/abstract=2472413 or http://dx.doi.org/10.2139/ssrn.2472413, at 10. See also: Westmoreland, Kate and Kent, Gail, International Law Enforcement Access to User Data: A Survival Guide and Call for Action (January 8, 2015). Available at SSRN: http://ssrn.com/abstract=2547289 orhttp://dx.doi.org/10.2139/ssrn.2547289.

Furthermore, a harmonisation of approach to statutory interpretation in this context necessarily invokes the need for uniformity of approaches in procedure. This, of itself will make MLAT requests or global warrant enforcement more efficient. Here we return to our investment or investment fraud example above. If these issues in relation to evidential collection are not effective then all that can be done is to investigate individual actors within a particular jurisdiction relying on requests from other countries with different and often lengthy procedures. This means that, if the hub of the activity is extraterritorial, then those at the top of a transnational enterprise will escape the scrutiny that comes with litigation or criminal prosecution. Victims will find that crimes go unpunished and genuine litigants will find no one to sue. The idea of global cooperation in such a context is of course likely to take a long time to develop and resolve. Given the recent conduct of the US in a surveillance context there is inevitable fear that one super power will use such an approach to ride rough shod over other national interests. Whilst the conversation on these issues has started in the context of the Microsoft case, we suggest there are other practical solutions which can be achieved in a swifter timescale. These can include uniformity of legal definitions and uniformity of police procedure thus reducing arguments on extradition as to whether an act in one country is defined in the same way in another and ensuring that evidence is collected properly in accordance with uniform procedures in each country – here we can think of collecting police confessions or downloading material using methods that are reliable and admissible in court. Such practicalities also then avoid arguments that evidence collected across nations then becomes inadmissible because the method of collection is considered improper in the country that has the nexus for prosecutorial jurisdiction. Super principles across jurisdictions will fail if basic methodology is unreliable. Such issues arise not just in relation to Internet intermediaries but particularly those involved in combatting transnational organised crime. Here the issue is not so much the proper law for the conduct of litigation but the collection of relevant evidence across territorial borders.

4.2. *Access through service providers*

Tying questions of jurisdiction exclusively to the location of the server has never been a good idea, and here, we want to outline a possible alternative. To prepare ground for that, it is useful to bear in mind that while Microsoft is one of the parties, the real dispute in the case is, as has been noted above, actually between U.S.'s claims of jurisdiction in the law enforcement setting on the one hand, and European data privacy values on the other. Thus, we must analyse both the U.S. standpoint and that of the EU.

The position of the U.S. Government is summarised in a statement made in its brief:

> *[T]he SCA [Stored Communications Act] warrant at issue does not involve any "extraterritorial application" of U.S. law. Instead, as Judge Francis held, the law is being applied exclusively within the United States—to a domestic provider [Microsoft] served within U.S. territory and subject to the personal jurisdiction of the issuing court. […] The fact that a provider may need to retrieve records from abroad in order to do so, due to the provider's own record-keeping practices, does not render the SCA "extraterritorial."*[47]

In other words, as there is no 'boots on ground' in Ireland, there is no extraterritorial claim of jurisdiction. We do not agree with this narrow and outdated view of extraterritoriality. However, as illustrated above, there can be no doubt that the concerns the U.S. is seeking to address are very real.

The EU position in matters such as this has become increasingly clear over the discussions of its proposed data privacy Regulation. However, here, it is most convenient to analyse the *amicus* brief filed in the case by a Member of the European Parliament – Jan Philipp Albrecht. For example, Albrecht states that "The content of that [the relevant] email account is located inside the EU and the customer therefore must benefit from the protections of EU law".,[48] and that: "For U.S. law to treat data stored in Europe as if it were stored in the United States is a territorial encroachment without justification, and one which is exacerbated by the sharp differences in the legal status of personal data in the U.S. and the EU".[49]

From our perspective, views such as that 'if data is located inside the EU it *must* benefit from the protections of EU law' are too simplistic as a solution even if they arguably amount to a correct description of the legal landscape under current thinking. And indeed, in Albrecht's *amicus* we can find hints, be as it may unintentionally communicated hints, at a better approach.

In his *amicus* brief, Albrecht asserts that:

> *Even if, contrary to the Appellant's case, the warrant at issue is capable of applying to the content of the email account, this would nevertheless give rise to a conflict of jurisdiction. Microsoft would be required by the warrant, yet it is not permitted under EU law to transfer the contents of the email account to the U.S.*[50]

But such a conflict may of course have two causes. It may be caused by an insensitive approach to law enforcement jurisdiction by the U.S. as in this case. However, it may also be a result of overly broad jurisdictional claims by the EU's data privacy law. And, we suggest that typically such conflicts are results of a combination of both.

As a first step towards a balanced model allowing law enforcement access to data held overseas, it must be

[47] Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (1:13-mj-02814) at 18–19.

[48] Amicus Curiae Brief in Support of Appellant Microsoft Corporation by Jan Philipp Albrecht, Member of the European Parliament, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (No. 14-2985-cv) at 8.

[49] *Id.* at 10.

[50] Amicus Curiae Brief in Support of Appellant Microsoft Corporation by Jan Philipp Albrecht, Member of the European Parliament, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (No. 14-2985-cv) at 9.

acknowledged that the EU's jurisdictional claim, as expressed by Mr Albrecht, is exorbitant in that it does not correspond with the EU's legitimate interests. Given the fluidity of data storage, it is unnecessarily aggressive to argue that all data located in the EU must automatically be protected by EU data privacy law. The real interest can usefully be more narrowly defined as is hinted at by the following statements made in Mr Albrecht's *amicus* brief:

1. *The rules governing the handling of personal data in the EU reflect the high level of sensitivity on the part of EU citizens and regulators about the protection of personal data.*[51]
2. *European citizens are highly sensitive to the differences between European and U.S. standards on data protection.*[52]
3. *Since Ireland hosts many datacenters operated by corporate groups whose headquarters are located in the United States, the present case is relevant for a gigantic volume of data held on behalf millions of EU citizens.*[53]
4. *The European Parliament has already noted the practice whereby, for example, a U.S. prosecutor ignores the EU MLAT and seeks to compel the disclosure of personal data belonging to an EU citizen by a technology company.*[54]

All these statements refer to the interest of *EU citizens*. The focus of EU data privacy efforts is, or at least should be, primarily directed at the protecting the personal data of EU citizens and others with a strong connection to the EU, such as permanent residents that are not EU citizens. This sentiment is also found in a recent document released by the Article 29 Working Party: "Under EU law, everyone has a right to data protection. In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State".[55] Thus, where a U.S. law enforcement agency in compliance with U.S. law seeks the assistance of a U.S. Internet intermediary to access the personal data of a U.S. citizen and resident, the EU's interest in applying its data privacy law is perhaps minimal even where that data happens to sit on a server in e.g. Ireland.

In light of the above, rather than focusing exclusively on the location of the data in question, it makes sense to place *primary focus* on the nationality of the person the data relates to. At the same time, it must be remembered that an e-mail account will contain both sent and received e-mails. Thus, in a selection of cases, also the e-mail account of e.g. a U.S. citizen may have a strong e.g. EU connection justifying the application of EU data privacy law.

Consequently, a primary focus on the nationality of the person the data relates to may usefully be accompanied by some form of *interest* or *connection test* – where data held in the EU has a sufficiently strong connection to the EU, EU data privacy law should prevent U.S. warrant-based access to the data even where the e-mail account belongs to a U.S. citizen. In such cases, U.S. law enforcement agencies would have to rely on the MLAT system.

Furthermore, under any alternative to the MLAT system, access to data located overseas should obviously only be provided where the government seeking access has legitimate jurisdiction over the Internet intermediary it calls upon.

Finally, we may complicate the model in a number of ways. For example, we could also consider whether the structure should go beyond a primary focus on nationality in certain types of offenses, such as child abuse offenses. However, we will not pursue such alternatives further here.

One way to summarise, concretise, and hopefully clarify, the proposal outlined above, is to express it as a legal model rule. It could, for example, look like this:

> *Outside a Mutual Legal Assistance Treaty, an Internet intermediary may only disclose personal data it holds in one country, on behalf of its users, to a law enforcement agency in another country, where:*
>
> (a) *the disclosure is mandated by the laws of the country in which the law enforcement agency is based;*
> (b) *the country in which the law enforcement agency is based has legitimate jurisdiction over the Internet intermediary;*
> (c) *the person whose data the law enforcement agency is seeking access to is a national or permanent resident of the country in which the law enforcement agency is based; and*
> (d) *the personal data to be disclosed lacks a substantial connection to the country in which the data is held.*

The exact operation of this model will depend on how key terms, such as *legitimate jurisdiction* and *substantial connection* are defined. However, we hope that this proposal may represent a useful starting point for much needed discussions of this crucially important issue.

5. Concluding remarks

As is widely known, in the late 70's, the OECD developed guidelines on basic rules governing the transborder flow and the protection of personal data and privacy. The purpose was to "facilitate a harmonization of national legislations, without this precluding at a later date the establishment of an international Convention." The Guidelines are described as "minimum standards for adoption in domestic legislation … and … .capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level". Decades on, there remains no internationally accepted set of principles.[56] The global nature of the connected world creates

[51] *Id.* at 5.
[52] *Id.* at 8.
[53] *Id.*
[54] *Id.* at 10–11.
[55] Article 29 Data Protection Working Party, 'Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" - C-131/12' (2014) WP225, at 3.

[56] ILRC comparative research related to Cambodia's Cybercrime Law prepared for the ABA Justice Defenders Programme by Felicity Gerry QC and Catherine Moore and forthcoming article GLOBAL CYBERLAW AND HOW CAMBODIA EXPOSED THE DANGEROUS DRIFT AWAY FROM COMMON HUMAN RIGHTS STANDARDS also by Felicity Gerry QC and Catherine Moore.

a new global legal conundrum highlighted here by the *Microsoft* case. Cybercrime laws needs to balance international criminal law principles with competing issues of sovereignty in the context of the online global community. The political effect of such challenges means that there is a vital need to address these issues. Some states are directly censoring and controlling the Internet,[57] while others place the responsibility for enforcing the law in the hands of the trade organizations who stand to gain from their enforcement.[58] Recent research by one author here in relation to a draft Cybercrime law for Cambodia exposed a dangerous global drift by all States from the necessary common human rights standards in the context of global cyber law.[59] As we have demonstrated, issuing an "external" warrant to demand the contents of a foreign server is a potentially draconian power which has the potential to infringe the human rights of individual privacy and data protection. States commitment to common human rights standards requires the formulation of a balanced set of cyber laws and procedures to combat cybercrime and improve cyber security, without compromising human rights in all States. The international convention envisaged by the OECD in the context of privacy is a proposal made in the context of Cambodian criminal law that is equally relevant to the litigation involving Microsoft. And while a general international consensus on data privacy may be quite premature to date, the Microsoft case highlights a degree of urgency in finding a solution to access to extra-territorial evidence.

Dan Svantesson is Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Visiting Professor, Faculty of Law, Masaryk University (Czech Republic). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

Felicity Gerry QC holds a research active post at Charles Darwin University focussing on data and rights, particularly in the context of violence against women and girls and the rule of law online. She lectures in advanced crime and evidence and is Chair of the Research and Research Training Committee in the School of Law. She is called to the Bar in England and Wales and is also admitted to the Supreme Court of the Northern Territory of Australia. She has been recognised in Chambers and Partners as "*vastly experienced advocate noted for her experience in serious sexual cases, homicides and frauds*". She is co-author of The Sexual Offences Handbook (2nd Ed 2014) http://www.wildy.com/isbn/9780854901227/sexual-offences-handbook-law-practice-and-procedure-2nd-ed-hardback-wildy-simmonds-and-hill-publishing (accessed 19 April 2015). A full biography appears here: http://www.felicitygerry.com/ (accessed 19 April 2015).

[57] S.C.S 'Why South Korea is really an Internet dinosaur ' *The Economist Explains Blog*(10 February 2014) <http://www.economist.com/blogs/economist-explains/2014/02/economist-explains-3>.

[58] Ed Black, 'WCIT, TPP, Russia PNTR: Growing Recognition of Internet Freedom As A Trade Issue' *Forbes* (online) 19 December 2012, http://www.forbes.com/sites/edblack/2012/12/19/wcit-tpp-russia-pntr-growing-recognition-of-Internet-freedom-as-a-trade-issue/.

[59] Ibid n57.