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.