the global voice of the legal profession

Criminal Law and Business Crime Newsletter

Newsletter of the International Bar Association Legal Practice Division

VOLUME 8 NUMBER 2 SEPTEMBER 2015

A conference presented by the IBA Criminal Law Committee and the IBA Business Crime Committee, supported by the IBA Latin American Regional Forum

the global voice of the legal profession

19th Annual IBA Transnational Crime Conference

11–13 May 2016, Panama City, Panama

Topics include:

- 21st century financial crimes
- Criminal liability associated with regulated products
- Criminal offences in freedom of speech
- Cybercrimes, crypto currency and their real effects
- Migration crises/border issues in criminal liability
- Money laundering
- Political campaign donations and gratuities

FOR MORE INFORMATION AND TO REGISTER YOUR INTEREST VISIT
WWW.IBANET.ORG/CONFERENCES/CONF674.ASPX

IN THIS ISSUE

Contributions to this newsletter are always welcome and should be sent to Ivo Leenders and Niels van der Laan at:

Ivo Leenders
Hertoghs advocaten-belastingkundigen, Breda
leenders@hertoghsadvocaten.nl

Niels van der Laan
De Roos & Pen Criminal Defence Lawyers, Amsterdam
vanderlaan@deroosenpen.nl

International Bar Association
4th Floor, 10 St Bride Street
London EC4A 4AD
Tel: +44 (0)20 7842 0090
Fax: +44 (0)20 7842 0091
www.ibanet.org

Terms and Conditions for submission of articles

1. Articles for inclusion in the newsletter should be sent to the Newsletter Editor.
2. The article must be the original work of the author, must not have been previously published, and must not currently be under consideration by another journal. If it contains material which is someone else's copyright, the unrestricted permission of the copyright owner must be obtained and evidence of this submitted with the article and the material should be clearly identified and acknowledged within the text. The article shall not, to the best of the author's knowledge, contain anything which is libellous, illegal, or infringes anyone's copyright or other rights.
3. Copyright shall be assigned to the IBA and the IBA will have the exclusive right to first publication, both to reproduce and/or distribute an article (including the abstract) ourselves throughout the world in printed, electronic or any other medium, and to authorise others (including Reproduction Rights Organisations such as the Copyright Licensing Agency and the Copyright Clearance Center) to do the same. Following first publication, such publishing rights shall be non-exclusive, except that publication in another journal will require permission from and acknowledgment of the IBA. Such permission may be obtained from the Director of Content at **editor@int-bar.org**.
4. The rights of the author will be respected, the name of the author will always be clearly associated with the article and, except for necessary editorial changes, no substantial alteration to the article will be made without consulting the author.

This newsletter is intended to provide general information regarding recent developments in business crime and criminal law. The views expressed are not necessarily those of the International Bar Association.

From the Co-Chairs

Welcome to our Fall 2015 Newsletter. We welcome your thoughts on this edition and your ideas for the next. The IBA Criminal Law and Business Crime Committees are working hard in preparation for the upcoming IBA Annual Conference in Vienna on 4–9 October 2015, where we will be hosting an exciting selection of panels and an array of excellent speakers. Please see **www.ibanet.org/Conferences/Vienna2015.aspx** for more details. We are looking forward to seeing you in Vienna for a wonderful chance to network in a beautiful setting.

We are pleased to announce that the Transnational Crime Conference in Berlin this spring was a resounding success! We wish to thank everyone in the Criminal Law Committee and those in the Business Crime Committee for all of their hard work. We had many interesting panels on a variety of topics, and Berlin is a fantastic city. We hope to see you at our next Annual Transnational Crime Conference in Panama City, Panama 11–13 May 2016.

We would like to extend a warm welcome to the Cybercrime Subcommittee and the Crimes Against Women Subcommittee, both newly formed under the Criminal Law committee. Monty Raphael is the Chair of the Cybercrime Committee and Olufunmi Oluyede the Chair of the Crimes Against Women Subcommittee. Please contact either for ways to get involved in these exciting new subcommittees or with any questions. Both subcommittees have sessions scheduled in Vienna, and both are having meetings in Vienna.

Another newsletter will be published after the Vienna conference. Articles should cover issues involving international criminal law and be submitted to the newsletter editors of the Criminal Law and Business Crime Committees. We will be very pleased if you are able to contribute and, once again, to assist you. Below are some pointers on what is required:

- subject: an international crime related topic. It may be specific to your own country or international in content.
- length: 500–2000 words, although a little shorter or longer may be published at the editor's discretion and edited if necessary.
- format: please have a title, short paragraphs and regular headings.

Thank you in advance for your submissions.

See you in Vienna!

CRIMINAL LAW COMMITTEE

Mark Biros
Proskauer Rose LLP, Washington
mbiros@proskauer.com

Ben Rose
Hickman & Rose, London
brose@hickmanandrose.co.uk

BUSINESS CRIME COMMITTEE

Brian Spiro
BCL Burton Copeland, London
bspiro@bcl.com

Mark Rochon
Miller & Chevalier Chartered, Washington, DC
mrochon@milchev.com

Committee officers

CRIMINAL LAW COMMITTEE

Co-Chairs
Mark Biros
Proskauer Rose, Washington
mbiros@proskauer.com

Ben Rose
Hickman & Rose, London
brose@hickmanandrose.co.uk

Vice Chairs
Gregory Kehoe
Greenberg Traurig, Tampa
kehoeg@gtlaw.com

Enide Perez
Sjöcrona Van Stigt Advocaten, Den Haag
ep@svsadvocates.com

Matthew Reinhard
Miller & Chevalier Chartered, Washington
mreinhard@milchev.com

Secretary
Nathalie von Taaffe
Credit Suisse, Dübendorf
nathalie.vontaaffe@credit-suisse.com

Treasurer
Roberto Durrieu
Estudio Durrieu, Buenos Aires
ar@estudiodurrieu.com.ar

Regional Representative Europe
Sophie Scemla
Heenan Paris, Paris
sscemla@heenanparis.com

Regional Representative North America
David Porter
McCarthy Tetrault, Toronto
dporter@mccarthy.ca

Regional Representative South America
Juliana Miranda
TozziniFreire Advogados, São Paulo
jmiranda@tozzinifreire.com.br

Regional Representative Africa
Omotola Rotimi
Lagos State Ministry of Justice, Lagos
omotolarotimi@yahoo.co.uk

Regional Representative India
Siji Malayil
Siji Malayil Associates Advocates & Solicitors, Bangalore
sijimalayil@yahoo.com

Conference Quality Officer
Astrid Mignon Colombet
Soulez Lariviere & Associes, Paris
mignon@soulezlariviere.com

Conference Coordinator
Heiko Ahlbrecht
Wessing & Partner Rechtsanwälte mbB, Düsseldorf
ahlbrecht@strafrecht.de

Publication and Newsletter Editor
Niels van der Laan
De Roos & Pen Criminal Defence Lawyers, Amsterdam
vanderlaan@deroosenpen.nl

Young Lawyers Liaison Officer
Jonathan Mattout
Herbert Smith Freehills LLP, Paris
jonathan.mattout@hsf.com

Academic Liaison Officer
Arthur Rizer
WVU School of Law, Morgantown
arthur.rizer@mail.wvu.edu

Website Officer
Mauro Wolfe
Duane Morris, New York
mmwolfe@duanemorris.com

Regional Representative Asia General
Andrew Powner
Haldanes, Central
powner@haldanes.com

Regional Representative Eastern Europe
Janusz Tomczak
Wardynski & Partners, Warsaw
janusz.tomczak@wardynski.com.pl

BUSINESS CRIME COMMITTEE

Co-Chairs
Fabio Cagnola
Studio Legale Bana, Milan
fc@studiobana.it

Jan Handzlik
Handzlik & Associates, Los Angeles
jhandzlik@handzliklaw.com

Senior Vice Chairs
Frederick Davis
Debevoise & Plimpton, Paris
ftdavis@debevoise.com

Kenan Furlong
A&L Goodbody, Dublin
kfurlong@algoodbody.com

Vice Chairs
Alexander de Swart
Houthoff Buruma, 1082 MA Amsterdam
a.de.swart@houthoff.com

Jessica Parker
Corker Binning, London
jp@corkerbinning.com

Secretary
Jorge Nemr
Leite, Tosto e Barros Advogados, São Paulo
jorgen@tostoadv.com

COMMITTEE OFFICERS

Treasurer
Janet Irene Levine
Crowell & Moring, Los Angeles
jlevine@crowell.com

Regional Representative Europe
Roger Burlingame
Kobre & Kim, London
roger.burlingame@kobrekim.co.uk

Regional Representative Europe
Aaron Stephens
Berwin Leighton Paisner, London
aaron.stephens@blplaw.com

Regional Representatives Latin America
Pierpaolo Bottini
Bottini & Tamasauskas Advogados, São Paulo
pierpaolo@btadvogados.com.br

Marcos Ríos
Carey, Santiago
mrios@carey.cl

Regional Representatives North America
William Devaney
Baker & McKenzie, New York
william.devaney@bakermckenzie.com

Nicholas Dunne
Walkers, George Town
nick.dunne@walkersglobal.com

David Martin
Martin and Associates, Vancouver
dm@martinandassociates.ca

Juan Torres-Landa
Hogan Lovells, Mexico City
juanf.torreslanda@hoganlovells.com

Regional Representative South America
Cristian Francos
Lewis Baach, Buenos Aires
cristian.francos@lewisbaach.com

Publications Officer
Kai Hart-Hoenig
Dr Kai Hart-Hoenig Rechtsanwälte,
Frankfurt am Main
kai.hart-hoenig@hart-hoenig.com

Newsletter Editor
Ivo Leenders
Hertoghs advocaten-belastingkundigen, Breda
leenders@hertoghsadvocaten.nl

Membership Officer
Elizabeth Robertson
K&L Gates, London
elizabeth.robertson@klgates.com

Conference Quality Officer
Dennis Boyle
Fox Rothschild LLP, Washington
dboyle@foxrothschild.com

Conference Coordinator
Sophie Scemla
Heenan Paris, Paris
sscemla@heenanparis.com

Corporate Counsel Forum Liaison Officer
Maurice Martin
Withers, London
maurice.martin@withersworldwide.com

Website Officer
Leila Babaeva
Miller & Chevalier Chartered, Washington
lbabaeva@milchev.com

Website Officer
Sonja Maeder Morvant
Lalive, Geneva
smaedermorvant@lalive.ch

Regional Representative Western Europe
Paul Gully-Hart
Schellenberg Wittmer, Geneva
paul.gully-hart@swlegal.ch

Regional Representative Asia General
James H M McGowan
Central
jhmmcg@hotmail.com

Regional Representative Western Europe
Roberto Pisano
Studio Legale Pisano, Milan
robertopisano@pisanolaw.com

Regional Representative Asia General
Akihisa Shiozaki
Nagashima Ohno & Tsunematsu, Tokyo
akihisa_shiozaki@noandt.com

Vienna 4–9 October 2015
ANNUAL CONFERENCE OF THE INTERNATIONAL BAR ASSOCIATION

Criminal Law and Business Crime Committee sessions

Monday 0930 – 1230

What were you thinking? The criminal trial of a multinational company and its CEO on corruption and fraud charges

Presented by the Criminal Law Section

Session Co-Chairs
Jan Handzlik *Handzlik & Associates, Los Angeles, California, USA; Co-Chair, Business Crime Committee*
Ben Rose *Hickman & Rose, London, England; Co-Chair, Criminal Law Committee*
James Tillen *Miller & Chevalier Chartered, Washington, DC, USA; Co-Chair, Anti-Corruption Committee*

This interactive criminal trial looks at the potential liability of a corporation and its CEO, charged with numerous counts of foreign bribery, conspiracy, money laundering and criminal breach of trust. The session will examine key issues of:

- the jurisdiction of the Austrian courts over foreign corporations and their officers;
- the criminal liability of a corporation and the role of the 'responsible corporate officer' doctrine;
- the liability of a corporation and its CEO for conduct of foreign subsidiaries and their agents;
- the availability of plea bargaining to reduce or eliminate the criminal exposure of the corporation and/or corporate officers; and
- avoiding the unexpected: anticipating and responding to parallel criminal and regulatory proceedings in multiple jurisdictions.

Speakers
Christine Braamskamp *K&L Gates, London, England*
Otto Dietrich *Dietrich RA, Vienna, Austria*
Friedrich Forsthuber *Vienna Criminal Court, Vienna, Austria*
Helene Gnida *Regional Criminal Court of Vienna, Vienna, Austria*
Patricia Kaindl *Vienna Public Prosecutor's Office, Vienna, Austria*
Janet Irene Levine *Crowell & Moring, Los Angeles, California, USA; Treasurer, Business Crime Committee*
Judge Stephanie Öner *Vienna Criminal Court, Vienna, Austria*
Stephen Pollard *WilmerHale, Oxford, England*
Volkert Sackmann *Vienna State Prosecutor Office, Vienna, Austria*

Coaches to the Landesgericht für Strafsachen Wien will depart from the main entrance of the Austria Center Vienna at 0915, and returning to the Austria Center Vienna at 1245.

Alternatively, the two nearest underground stations for the Landesgericht are Rathaus and Schottentor on the line 2.

LANDESGERICHT FÜR STRAFSACHEN WIEN,
LANDESGERICHTSSTRASSE 11, 1080 VIENNA

Monday 1430 – 1545

IBA and *Equality Now* rape laws crowdsourcing project: final report

Presented by the Criminal Law Committee, the Family Law Committee and the Crimes Against Women Subcommittee

Session Moderator
Jacqui Hunt *Equality Now, London, England*

The Criminal Law and Family Law Committees have been working hard throughout the year with *Equality Now*, an organisation advocating for the human rights of women and girls. A global database of rape laws was created to determine how rape is defined in different countries and to identify best practice guidelines. Jacqui Hunt of *Equality Now* will present the findings of this comprehensive and ambitious research project. The report will be followed by a discussion on current harmful and discriminatory provisions in various states and will address ideas for engendering change.

Speakers
Ruwani Dantanarayana *John Wilson Partners, Colombo, Sri Lanka*
Olufunmi Oluyede *TRLPLAW, Lagos, Nigeria; LPD Council Member*
Gillian Rivers *Penningtons Manches, London, England; Chair, Family Law Committee*
Meg Strickler *Conaway & Strickler, Atlanta, Georgia, USA; IBA Liaison Officer, War Crimes Committee*

HALL L1

Tuesday 0930 – 1230

A firm hand on the tiller – steering your client through the choppy waters of a major corporate crisis

Presented by the Business Crime Committee

Session Co-Chairs
Kenan Furlong *A&L Goodbody, Dublin, Ireland; Senior Vice Chair, Business Crime Committee*
Mark Rochon *Miller & Chevalier Chartered, Washington, DC, USA*

This panel will offer practical guidance on how to manage the legal, operational and reputational aspects of a major corporate crisis. It will feature lawyers and a crisis communications expert who have advised

Continued overleaf

on some of the world's most high-profile recent corporate crises. Issues covered will include:

- communications with staff, customers, insurers, regulators, the market and the media;
- the paper trail – document creation and retention;
- the investigation – who should do it? How should they do it?
- getting the right report; and
- the aftermath – dismissals, civil actions, remedial steps. When and how do you 'draw a line'?

Speakers
Michael Carney *FleishmanHillard, Brussels, Belgium*
Carlos da Silva Ayres *Trench Rossi e Watanabe Advogados, São Paulo, Brazil*
Andrew Kaufman *Andrew Kaufman, New York, USA*
Astrid Mignon Colombet *Soulez Lariviere & Partners, Paris, France; Conference Quality Officer, Criminal Law Committee*
Stephen Parkinson *Kingsley Napley, London, England*

ROOM -2.31

Tuesday 1615 – 1730

Cybercrime: its current manifestations

Presented by the Cybercrime Subcommittee, the Criminal Law Committee and the Technology Law Committee

Session Moderator
Meg Strickler *Conaway & Strickler, Atlanta, Georgia, USA; IBA Liaison Officer, War Crimes Committee*

The panel will discuss how the cybercrime threat, both public and private, is emerging and being confronted domestically and internationally.

Speakers
Árpád Geréd *Maybach Görg Lenneis, Vienna, Austria*
Monty Raphael QC *Peters & Peters, London, England; Chair, Cybercrime Subcommittee*
Juliana Miranda *Tozzini Freire Advogados, São Paulo, Brazil; Representative South America, Criminal Law Committee*

HALL K1

Wednesday 0930 – 1230

Apple Pay, Bitcoin, a cashless society: discussion on legal issues in mobile payments and digital currencies

Presented by the Leisure Industries Section, the Banking Law Committee, the Criminal Law Committee, the Cybercrime Subcommittee, the Intellectual Property and Entertainment Law Committee and the Technology Law Committee

2015 will see continued shifts in mobile payments and virtual currencies along with the move to a society that uses less and less cash. Come and discuss the year in review for digital money with our engaging panels. Has Apple Pay or the Google Wallet changed the payments landscape or the security landscape? Will the continued expansion of EMV chip cards in the US have an impact? And what has happened with Bitcoin and the blockchain? What changes does the expansion of the BTC protocol and the blockchain foreshadow for FinTech?

Speaker
Brian Klein *Baker Marquart, Los Angeles, California, USA*

Panellists
Marcus Clinch *Eiger Law, Taipei, Taiwan*
Andreas Leupold *Munich, Germany; Secretary, Electronic Entertainment and Online Gaming Subcommittee*
Gabrielle Patrick *Epiphyte, London, England; Chair, Electronic Entertainment and Online Gaming Subcommittee*
Arthur Stadler *Brandl & Talos Attorneys at Law, Vienna, Austria*
Gil White *Herzog Fox & Neeman, Tel Aviv, Israel*

HALL L7

Wednesday 1430 – 1730

Tax planning structures and cross-border transactions: criminal implications for the members of the corporate bodies and for the external advisers in case of tax audit

Presented by the Business Crime Committee and the Taxes Committee

Session Co-Chairs
Fabio Cagnola *Studio Legale Bana, Milan, Italy; Co-Chair, Business Crime Committee*
Enrique Calvo-Nicolau *Calvo Nicolau y Márquez Cristerna-DFK, Mexico City, Mexico*

What happens when tax auditors redefine a tax planning structure? The session will explore the tax and criminal implications that may affect the members of the corporate bodies and tax advisers who have devised the structure and participated in its implementation.

Speakers
Kevin Downing *Miller & Chevalier Chartered, Washington, DC, USA*
Marc Henzelin *Lalive, Geneva, Switzerland*
Riccardo Michelutti *Maisto e Associati, Milan, Italy*
Panagiotis Pothos *Kyriakides Georgopoulos Law Firm, Athens, Greece*
Diego Salto *AFC, San Jose, Costa Rica*
Dariusz Wasylkowski *Wardyński & Partners, Warsaw, Poland*

ROOM -2.31

Thursday 0930 – 1230

Inherent and subsequent risk: criminal liability for individuals and entities arising out of mergers and acquisitions

Presented by the Criminal Law Committee, the Business Crime Committee and the Corporate and M&A Law Committee

Session Co-Chairs
Mark Biros *Proskauer Rose, Washington, DC, USA; Co-Chair, Criminal Law Committee*
Finn J Lernø *Plesner, Copenhagen, Denmark; Membership Officer, Corporate and M&A Law Committee*

This panel of criminal law and corporate law experts experienced in M&A activity will analyse situations from various jurisdictions where criminal liability and serious quasi-criminal enforcement issues have arisen out of mergers – both successful and failed. A multinational hypothetical case will provide a basis for discussion. Topics will include how, if at all, a jurisdiction's legal obligation to report crime may impact a deal, the increased necessity of 'legal compliance' due diligence, the role, if any, of a criminal attorney in due diligence once issues arise, how deals create/defeat successor liability, fraud in valuations, individual and organisational liability, generally, and measures to mitigate or reduce risk. Part one of the session will address issues from the perspective of prior to completion of the deal; whereas part two will analyse defending against allegations of wrongdoing that are lodged after the deal is done.

Speakers
Heiko Ahlbrecht *Wessing & Partner Rechtsanwälte, Dusseldorf, Germany; Conference Coordinator, Criminal Law Committee*
Audry Li *Zhong Lun Law Firm, Shanghai, China*
Mark Mendelsohn *Paul Weiss Rifkind Wharton & Garrison, Washington, DC, USA*
Fabyola Rodrigues *Demarest Advogados, São Paulo, Brazil*
Ben Rose *Hickman & Rose, London, England; Co-Chair, Criminal Law Committee*
Gisèle Rosselle *Strelia, Brussels, Belgium*

ROOMS 1.85 & 1.86

Thursday 1330 – 1430

Open committee business meeting

Presented by the Criminal Law Committee

An open meeting of the Criminal Law Committee will be held to discuss matters of interest and future activities.

ROOMS 1.85 & 1.86

Thursday 1430 – 1730

Policing the world: the role of national courts in extra-jurisdictional conflict crime

Presented by the Criminal Law Committee and the War Crimes Committee

Session Co-Chairs
Jonathan Grimes *Kingsley Napley, London, England; Co-Chair, War Crimes Committee*
Matthew Reinhard *Miller & Chevalier, Washington, DC, USA; Vice Chair, Criminal Law Committee*

Conflicts taking place abroad are ever more the business of national courts. Whether these are prosecutions of nationals who have gone abroad to fight for financial or ideological motive, or result from the operation of universal jurisdiction in respect of war crimes offences, a range of legal, practical, and ethical issues arise. Looking at such prosecutions in a number of jurisdictions around the world the session will look at issues such as:

- differing approaches to the jurisdiction of national courts for offences committed abroad;
- the not so universal approach to universal jurisdiction cases;
- the politics behind the decision to prosecute – why some but not others? and
- practical problems prosecuting offences where the evidence is all abroad.

Speakers
Jeremy Gauntlett SC *General Council of the Bar of South Africa, Cape Town, South Africa*
Daniel Machover *Hickman & Rose, London, England*
Michiel Pestman *Prakken d'Oliveria Human Rights Lawyers, Amsterdam, the Netherlands*
David Schertler *Schertler & Onorato, Washington, DC, USA*
Natalie von Wistinghausen *NVW Law, Berlin, Germany*
Alain Werner *Civitas Maxima, Geneva, Switzerland*

ROOMS 1.85 & 1.86

FEATURES

The problem of financing election campaigns in Brazil

BRAZIL

Vânia Aieta

Rio de Janeiro State University and Siqueira Castro Advogados, Rio de Janeiro

vaniaaieta@siqueiracastro.com.br

Introduction

In this article I argue that exclusive public financing of elections is not necessarily the best option for Latin America. I cover the most relevant points of exclusively public, exclusively private and mixed financing, to demonstrate that the radical choice of the exclusively public model will not resolve the current demands of societies. The focus is on Brazil, where private financing has been accused of being responsible for corruption. In counterpoint, I demonstrate that the problem is not private funding per se, but rather failure of rigorous transparency and rendering of accounts.

'Money, like water, will always find an outlet.'

Justice John Paul Stevens
US Supreme Court Justice from 1975–2010

The Brazilian social imagination in recent years has continued to be stirred up by corruption scandals and political mudslinging, something that has haunted Brazilian political life for generations. While in many cases these accusations have proved to be true, it should not be forgotten that the moralistic tone of calls to 'clean up' politics is partly a reaction of more conservative elements against the return of democracy in 1985, after two decades of military dictatorship. Therefore, while calls to clean up politics are laudable, one must not lose sight of the overarching importance of the free exercise of political rights.

Brazil's political institutions are still paying a heavy price for the years of dictatorship, which among other negative legacies has made political institutions as a whole more fragile – most notably the weak and fractured system of political parties which should be the repositories of social demands. Other aspects of this institutional fragility are the promiscuity and absence of strong ideologies in political relations, with pragmatism and patronage reigning supreme, as well as the lack of transparency, control and credibility regarding the financing of political campaigns and parties, despite the more efficient work of the public prosecutors, audit tribunals and electoral courts.

Of course, this is not only a Brazilian problem. All countries, no matter their governing system, suffer from political corruption to one degree or another. But there is growing awareness in the world that corruption generates inefficient allocation of resources and deteriorates the quality of public services as it not only diverts tax revenue into private hands, it also creates incentives for misguided spending.

Although all corrupt conduct is illegal, the fight against it should not be allowed to serve as a justification for disrespecting constitutional precepts.

Finally comes the change in the moral quality of the common citizen, which combined with inequality leads to the emergence of selfish political factions and interest groups or lobbies. Ironically, one of the problems in Brazil is that of misguided idealism: lobbying is seen as the exercise of undue influence over politicians rather than a normal part of the political process. As such, unlike in most other countries, in Brazil there are no rules to establish what lobbyists can and cannot do and no oversight of the activity.

The conflict among political factions and continued inequality allow the corruption on high to pass throughout society. Public officials pay lip service to the people while in reality they are more beholden to the classes represented by these political factions, generating a perverse situation of greater class polarisation. Hence, a social pyramid is entrenched with a privileged class enjoying full rights at the apex while the rest of the population, the mass of people, are robbed of their full rights as citizens.

The factionalism that marks Brazilian politics, with a surfeit of parties with weak ideals, hampers governability. While political

pragmatism certainly is preferable to rigid ideological purity, whereby compromise is impossible and results in stalemate, the weak ideology that typifies Brazilian parties means governability is only achieved through backroom deals and the exchange of favours through pork barrel politics, leading to coalitions formed of strange bedfellows. This deal-making inevitably transcends government, often being achieved though the intermediation of businesses.

One cannot overlook the existence of a strong connection between the moral and social requirements of a just and stable state and the question of social inequality, as empirically shown by the prevailing tendencies of current political life, among them the impotence of the poor and their precarious and intermittent political participation. With politics playing an important role in socialisation, the participation of all in the political process is necessary to maintain a healthy democratic order.

In contrast, the lack of participation leads to a corrupt state, marked by sharp inequality in the distribution of wealth, power and status. Moral rupture combined with inequality provides fertile ground for the development of factions that become centers of wealth and power and usurp the legitimate functions of government.

Looming over the political landscape, including the problem of political corruption, is the need to assure governability. This need is present in all political systems to a greater or lesser extent. The more fractious and numerous political parties are, the harder it will be to achieve a reasonable degree of governability. But even in the most stable democracies with the lowest levels of corruption, politics observed up close is a messy business, much like observing the operation of a sausage factory, to call on the old adage. Assuring governability as opposed to deadlock inevitably requires, to some degree, the exchange of political favours, often at the cost of technical (and moral) quality. The political game also inherently involves the influence of organised interest groups, be they NGOs, businesses, labour unions, etc, whether directly in the form of money or indirectly in the form of organisational support. Simply put, it takes money to run a successful political campaign, and a large part of that money will come from the organisations with the strongest interest, for economic, moral or other reasons.

Private financing of political parties is often held up as the great villain, responsible for all the corrupt practices in raising funds for election campaigns, with public funding of parties being proposed as the great panacea. This is an overly simplistic view.

Brazil has a mixed system of financing political parties and election campaigns, conciliating private donations with government subsidies. Nevertheless, there was a movement to shift to a system of sole public funding.

As stated, in Brazil private financing has been indicated as the main culprit for political corruption. But I assert that the best way to control corruption is through effective transparency and oversight of accounts. Blaming the method of campaign financing for corruption only serves to divert attention from the real villains, those who abuse the existing system, and who would likely do the same under a purely public financing regime. In short, private financing is not responsible for corruption. That responsibility rests with the corrupt politicians and public officials.

Furthermore, the possibility of making donations to candidates and parties is a legitimate political right of all citizens, a right that is a sub-type of human rights, inalienable, a main pillar of the realisation of the democratic principle.

This right of citizens cannot be constrained only to the act of voting. After all, it is naive to think that politics can be conducted without financing. Citizens have the right to contribute to the candidates and parties of their choice. And this right must also be extended to corporate citizens in the broad sense. It must be recalled that political parties themselves are legal entities. Parties are the genuine repositories of the desires of society.

There is nothing wrong with advocating a political position that, if translated into law, would financially benefit a particular person or group of persons. The press is for the most part not neutral, nor are companies or interest groups. If there were neutrality, politics would not exist in the first place. Politics is the game of establishing public policies based on competition between the ideological, moral, and yes, economic positions of non-neutral players. What is necessary is to establish effective transparency and control by allowing voters to know, with the assistance of gatekeepers like audit tribunals and electoral courts, what parties and candidates are receiving financial support from which sources, so that voters can factor this information into their decisions.

Besides this, Brazil already has sufficient legal and accounting mechanisms and instruments for control and oversight of the fundraising by candidates and parties. This is established by the Brazilian Election Law, all candidates are responsible for the veracity of the information reported, with the financial management of campaigns being carried out by the candidate himself/herself or a trusted appointee (usually an accountant of lawyer).

The fact that election financing is through parties rather than the independent fundraising efforts of candidates is basis for the rule against switching parties after the election. The idea is that the seat or executive position belongs to the party rather than the elected official. While this system has the positive effect of discouraging opportunistic party-hopping during legislative sessions, thus making it easier to maintain the political coalitions necessary for governability in a system where no single party can marshal enough support to govern alone, it has the drawback of making it virtually impossible for a truly independent candidate to get elected.

The debate over campaign financing cannot ignore the fact that the government has a significant presence in the nation's economy, directly through outright ownership or control of large companies in key sectors such as petroleum, electricity generation and banking, and indirectly through subsidies and tax exemptions in areas such as housing and shipbuilding (not to mention the traditional public services like health, education and sanitation). Indeed, estimates are that nearly two-thirds of economic activity to some extent depends on the government, either directly through State control or in the form of low-interest public loans, subsidies and tax exemptions/benefits. In a setting like this, it is unreasonable not to allow businesses to exercise influence through political contributions in the so-called 'government market'.

Since political parties represent sectors of society, it is reasonable to allow their financing to come from other players of organised civil society, not only the government. This does not mean laissez-faire financing, because the Constitution determines the suppression of abuse of economic and political power, and candidates and parties are already required to render accounts to the electoral courts.

There are only three ways of financing political parties and campaigns:

- public financing (direct and/or indirect);
- private financing; and
- mixed financing.

The main argument of proponents of public financing is that it will reduce corruption. This is mainly a rallying cry of the parties of the left, because they claim they tend to attract less funding from corporate sources. The argument goes that having to compete in the marketplace for campaign financing forces leftist candidates to forgo their ideals. This is a fragile argument because big donor money in Brazil goes to politicians of all political stripes.

The best alternative is the middle ground of a mixed financing system, as exists in the United States and many countries in Latin America with similar coalition presidential systems as Brazil's. The main argument in favour of this system is its dispersion of funding sources, so that political parties will not be overly beholden to private interests or too reliant on taxpayer money. And companies should be able to participate in the financing of elections, since they are legal persons that pay taxes and have legitimate interests to pursue in the forum of political action.

Besides the relevant legal arguments against forbidding corporate citizens from making political donations, there is the pragmatic one that exclusive public funding already proved inefficient in the past in Brazil, only driving financing into the shadows. It would be a step backward to the days of authoritarian presidentialism and an economy mainly in the hands of the state, with power concentrated in the hands of the few.

On this matter, the decision of the United States Supreme Court in *McConnell v Federal Election Commission* placed limits on financing by corporations, unions and wealthy individuals but recognised the right of corporate entities to support political parties and candidates. This is exactly what is needed in Brazil: an effectively overseen and enforced system of mixed financing. The attempt to outlaw private financing of political parties and candidates may be more egalitarian in principle, but in practice it does not work because it runs counter to the system of free enterprise. As noted by Justice John Paul Stevens: 'Money, like water, will always find an outlet.'

ITALY

Emilio Battaglia
CMS Italy
emilio.battaglia@cms-aacs.com

Bill no 69/2015 concerning 'Provisions on offences against public administration, mafia conspiracies and false corporate disclosures'

Abstract

The new Bill no 69/2015 (the 'Bill') provides:

- the increase of penalties for some offences against the Public Administration and the offence of 'Mafia conspiracies including foreign';
- amendment to the offence of 'Extortion';
- the introduction of a new mitigating circumstance and monetary compensation in respect of the Administration;
- modification to the provisions of the suspension of penalties and the plea bargain;
- reinforcement of the role of the National Authority for Anti-Corruption (ANAC);
- reform of the accounting frauds; and
- amendments to section 25 *ter* of Legislative Decree no 231/2001, concerning corporate offences.

On 21 May 2015, the Chamber of Deputies gave approval to the Bill, concerning 'Provisions on offences against public administration, mafia conspiracies and false corporate disclosures'.

The Bill was published in the Italian Official Journal on 27 May 2015 and became effective on 14 June 2015. The Bill is aimed at introducing a series of amendments, in particular with regard to offences against the Public Administration and accounting frauds.

As for the new provisions regarding offences against the Public Administration, first the increase of additional and principal penalties provided by the following offences should be noted: 'misappropriation' (under section 314 of the Italian Criminal Code); 'bribery in the exercise of the functions' (under section 318 of the Italian Criminal Code); 'bribery to obtain an act contrary to official duties' (under section 319 of the Italian Criminal Code); 'bribery in judicial acts' (under section 319 *ter* of the Italian Criminal Code); 'improper inducement to give or promise a benefit' (under section 319 *quarter* of the Italian Criminal Code).

Furthermore, this regulatory action is of significant interest because the Italian Legislator has amended the offence of 'extortion' ('*Concussione*'), punishable under section 317 of the Italian Criminal Code, by extending responsibility under the offence to include, in addition to public officials, people in charge of public service.

Among the other changes envisioned by the Bill, with reference to crimes against the Public Administration, the introduction of a new hypothesis of mitigating circumstances (specifically, the new second paragraph of section 323 *bis* of the Italian Criminal Code, which provides for a reduction of the sanctions for individual offenders who effectively strive to avoid corruption activities which produce further illicit consequences, or to those who effectively cooperate in gathering evidence and identifying other offenders), and the institution of monetary compensation in respect of the Administration injured by the offence (provided for in the new section 322 *quarter* of the Italian Criminal Code), should also be noted.

The Italian Legislator has also amended some provisions of the Italian Criminal Procedure Code – in particular, section 165, concerning the suspension of penalties; and section 444, with reference to the plea bargain – and consideration should be made to these amendments.

In addition, the Italian Legislator has modified some provisions of Law no 190/2012 (on 'Provisions for the prevention and repression of corruption and illegality in the public administration') and has reinforced the role of ANAC, in particular, requiring the Public Prosecutors to inform ANAC in cases of prosecution for crimes

against the Public Administration.

However, Law no 69/2015 provides a general increase of the penalties provided for the offence of 'Mafia conspiracies including foreign' pursuant to section 416 *bis* of the Italian Criminal Code.

Among the other main innovations, there has been reform of the accounting frauds: indeed, false corporate disclosure returns are now to be expected as an offence in relation to all companies, not only in relation to quoted companies.

In detail, the reform consists of a complete review of sections 2621 and 2622 of the Italian Civil Code. As a result of the amendments, the offence of false accounting punishes directors, officers, statutory auditors and liquidators who, in order to achieve an illicit profit, either provide false information or omit information prescribed by law, in balance sheets, corporate reports or other communications. Furthermore, Law no 69/2015 eliminates the non-liability clauses for non-material omissions and introduces reduced sanctions for lesser offences in the new section 2621 *bis* of the Italian Civil Code.

Finally, the amendments in the matter of 'Administrative responsibility of entities' pursuant to Legislative Decree no 231/2001 should be noted. In particular, section 25 *ter* of Legislative Decree no 231/2001, concerning corporate offences: (1) eliminated the limitation provided for in the first paragraph, letter *a)*, regarding the possible responsibility for the crime (directors, general managers, liquidators or persons subject to their supervision); (2) with regards to the offence under section 2621 of the Italian Civil Code, elevated the maximum fine applicable to companies in the case of conviction from 300 to 400 quotas (while the minimum fine of 200 quotas remains the same); (3) introduced the new letter *a) bis* in the first paragraph, as a result of the introduction of the new section 2621 *bis* of the Italian Civil Code (false corporate disclosures of low relevance in unquoted companies), providing for, in relation to this offence, the application of a fine from 100 to 200 quotas; (4) changed the letter *b)* of the first paragraph, by introducing a reference to the new offence of false corporate disclosures of quoted companies, with the application of a fine from 400 to 600 quotas.

The corporation and the right to remain silent

NETHERLANDS

Ivo Leenders

Hertoghs advocaten-belastingkundigen, Breda & Rotterdam

leenders@hertoghsadvocaten.nl

Judith de Boer

Hertoghs advocaten-belastingkundigen, Breda & Rotterdam

boer@hertoghsadvocaten.nl

In the Netherlands, Article 51 of the Criminal Code provides for criminal liability of legal entities and its officers or principals. This form of criminal liability was introduced into the Criminal Code in 1976.[1] The two recurring questions in the Dutch legal system are:

- what is the scope of the right to remain silent of a legal entity?; and
- how should the judiciary deal with the rights of employees of a company?

In introducing the Bill that included Article 51 of the Criminal Code, just – although little – attention has been paid to the duty to testify of the representatives of the legal entity. The following is noted about this – relating to Article 528 of the Code of Criminal Procedure – in the explanatory memorandum:[2]

> 'When the personal appearance of a director has been ordered in a criminal case against a legal entity under the proposed Article 528, he will not be able to act as a witness in the criminal case against the legal entity. He is, after all, supposed to represent the corporation, which excludes that he could testify against or in favour of it.' (free translation)

From this phrase it could be concluded that only the representative of the legal entity has the right to remain silent in the criminal investigation. However, this does not seem sufficient to secure the right to remain silent of the accused legal entity.

The Supreme Court confirmed in 1993 that the guarantees of Article 6 of the European Convention for the Protection of Human Rights also apply to the legal entity.[3] The legal entity

thus has the right to remain silent. However, since the legal entity has no voice and in this regard is not able to make any personal statement, who is entitled to this right?

To our knowledge, the Supreme Court has so far only passed a judgement regarding the representative's right of the legal entity to remain silent.[4] It follows from Article 528 of Code of Criminal Procedure that the (actual) directors of the legal entity may act as representative. The lower Federal Court case law[5] has held that in a general sense the employees of an accused legal entity do not have the right to remain silent.

The question is whether this judgment is correct. In our view, the scope of the right to remain silent should be adapted to the scope of criminal liability per se. After all, as much as a legal entity does not have a voice it can also not act or omit independently while it can commit a criminal offence.

The capacity of a legal entity to be an offender is by its very nature an author in an organisation context. It is a person's actions or omissions which are attributed to the legal entity, being the acts of the legal entity itself. The Supreme Court held that it is decisive for the criminal liability of a legal entity whether the relevant practice may be reasonably attributed to the legal entity.[6] That is, according to the Supreme Court, particularly the case if such practice occurs within the sphere of the legal entity.

Attributing actions or omission to a legal entity therefore takes place in the broadest sense of the word. Actions or omissions of the employees of the legal entity may result in criminal liability of the legal entity. On that basis it would advocate that anyone acting in the sphere of the legal entity has a right to remain silent when the legal entity is suspected of a criminal offense.

A similar result is found in competition law. The basic thinking of Article 53 of the Competition Act is the guiding principle that companies are not obligated to make a declaration that (possibly) can be damaging to them.

The Regulatory Industrial Organisation Appeals Court considered the following:[7]

> 'In the case of *Texaco* (LJN AI1062) the Court has already held that it may not be inferred from the wording of Article 53 of the Competition Act nor the legislative history that the right of a company to remain silent is limited to a restricted circle of people. On the contrary, from the words 'on part of the company' the Court concludes that if the company is heard the right to remain silent is granted to anyone who belongs to that company; not just the civil representative(s) has the right to remain silent. It is therefore different from the situation where the employee directly as an individual, not on behalf of the Company, is asked to provide information.' (free translation)

Of course this rule is easy to avoid by asking each question directly without ensuring the question asked is in principle asked on behalf of the company. Therefore, employees of an accused legal entity should have, in principle, the right to remain silent. We fail to see why the interpretation of the right to silence under Article 29 of the Code of Criminal Procedure should be different from Article 53 of The Competition Act. We advocate a broad interpretation of the right to remain silent for the accused legal entity.

However, practice shows that this right is not respected by the investigative authorities. In financial criminal law, we often see that during a search of the company the Fiscal Information and Investigation Service (the 'FIOD') initially secures the documents and data. The next step is that employees or other persons present at the company are questioned without clarifying who is really representing the company or if questions are asked on behalf of the company.

Besides the discussion on the scope of the right to remain silent, these 'witnesses' are unaware of their rights as a witness. People are caught off guard as they often do not know that if they are heard as a witness there is no obligation (in the Netherlands) to talk to the FIOD or police. The employee therefor gets into a conflict. Frequently an employee of a company has a confidentiality clause in his contract. He may therefore not provide information voluntarily. This will be different if a witness statement is required by law. A witness is only legally required to (truthfully) explain to a judge. Under the guise of 'it's yours for asking', employees of companies accused are interviewed in a stressful situation – namely, just after the FIOD comes into play – without employees being aware of their rights.

In our view, this practice is not only contrary to the right to remain silent of the accused company, but clear rules should at least be reinforced regarding the approach of witnesses. In this way the power play of the FIOD does not discard the rights of witnesses. Just as the legal entity is responsible

for keeping its employees in line to avoid criminal liability, people who engage in activities in the sphere of the legal entity should enjoy the same rights as the legal entity. If not they should at least be informed about their rights as a witness.

We are very curious about the scope of the right to remain silent of the accused legal entity in other countries. Or is there an obligation to make witnesses aware of their rights in your country?

To share the requested information and/or for your queries, please contact Ivo Leenders and Judith de Boer. We can be reached at **leenders@hertoghsadvocaten.nl** and **boer@hertoghsadvocaten.nl**.

Notes

1 Official Journal of Laws (Staatsblad) 1976, 377.
2 Dutch House of Representatives, session 1975-1976, 13 655, nos 1–3, p 25.
3 Dutch Supreme Court, 1 June 1993, no 93971E, ECLI:NL:HR:1993:ZC9378.
4 Dutch Supreme Court, 13 October 1981, no 73063E, ECLI:NL:HR:1981:AC3210.
5 *Ibid.*
6 *Ibid.*
7 Regulatory Industrial Organisation Appeals Court, 21 December 2012, ECLI:NL:CBB:2012:BY7031.

Increased warfare: United States economic sanctions – beware of the pitfalls

UNITED STATES

Mark J Biros*
Proskauer Rose LLP, Washington
mbiros@proskauer.com

Tensions between the Russian Federation and the West are the worst since the Cold War. But instead of military thrusts and parries, economic sanctions are the weapons of choice. Russia has many fertile investment opportunities. It also ranks 128th out of 177 countries with perceived serious corruption problems. The volatile political climate has spawned sanctions on Russian nationals, banks and aspects of the Russian oil industry. While talk of loosening the sanctions against Cuba and Iran due to political issues has captured centre stage, the core sanctions against the two countries have actually changed little. Sanction provisions can be imposed quickly. They follow national political and security interests not business ones. Contravening them can cause serious adverse business consequences.

Recently, a Middle Eastern company drilling for oil in a Middle Eastern country using no US personnel was drastically affected by the sanctions. Its business operations were supervised by a Chinese company which hired a Sudanese business to provide services to the operations. The company received the Sudanese business' invoice seeking a 500,000 SDG payment. The Sudanese business then requested payment in US dollars. The company sent the invoice to its London bank with a request to pay it in US dollars. The London bank sent a request for dollars to BNY Mellon in New York City. When BNY Mellon saw the Sudanese business' name on the paperwork, it blocked the transaction and froze the Euros it received to cover the conversion. The Sudanese business was subject to US sanctions. BNY Mellon queried the London bank as to whether it had a licence for the transaction. The London bank did not. BNY Mellon blocked the transaction.

The Middle Eastern company never got its funds back even though it was a non-US company doing business outside the US without any US personnel. A foreign transaction ran afoul of the US economic sanctions solely because it involved a US bank in a minor role.

Tangential connections to the US can even create criminal liability. Earlier this year, Schlumberger Oilfield Holdings Ltd (SOHL), a wholly-owned British Virgin Island subsidiary of Schlumberger Ltd entered a guilty plea for conspiring to violate the International Emergency Economic Powers Act (IEEPA) by wilfully facilitating illegal transactions with Iran and Sudan.

It was lawful for SOHL, as a non-US entity, to operate in Iran and Sudan under certain circumstances, and SOHL had policies to ensure the company did not violate US economic sanctions. However, employees of Drilling & Measurements (D&M), a Texas-based Schlumberger business segment which

provided services to SOHL were not trained adequately to ensure that all company US persons, including non-US citizens who resided in the US while employed by D&M complied with those policies. What did the employees do? They provided normal business services to SOHL for its Iranian and Sudanese operations by:

- approving and disguising SOHL's capital expenditure requests from Iran and Sudan for the manufacture of new oilfield drilling tools and for the spending of money for certain company purchases;
- making and implementing business decisions specifically concerning Iran and Sudan; and
- providing certain technical services and expertise to troubleshoot mechanical failures and to sustain expensive drilling tools and related equipment in Iran and Sudan.

This involvement of US persons rendered criminal transactions that if done by SOHL alone would not have violated US law. Because D&M was working with SOHL, the government charged SOHL, a foreign entity, with conspiracy to violate the IEEPA under 18 USC § 371, the federal conspiracy statute. SOHL was required to forfeit US$77,569,452 in proceeds from the offence and pay a criminal fine of US$155,138,904, all of this because it failed to monitor the involvement of a US business segment in its global operations.

US economic sanction programme

The Office of Foreign Assets Control (OFAC) administers US economic sanctions targeting entities, nationals, governments, geographic regions and market sectors. Sanctions are directed at Cuba, Iran, Russia, Sudan, and Syria plus the Western Balkans, Belarus, Cote d'Ivoire, Democratic Republic of the Congo, Lebanon, Liberia, North Korea, Somalia, Ukraine, and Zimbabwe. Nationals of, or entities located in, or those working on behalf of persons or entities connected to, these countries, directly or indirectly, are covered. A Specially Designated Nationals and Blocked Persons (SDN) list identifies parties connected with sanctioned activities with, or in locations in, which no US person may transact business.

Three Presidential Executive Orders have been issued sanctioning persons and entities contributing to the turmoil in the Ukraine. A Sectoral Sanctions Identification (SSI) list has been created. Four Directives were promulgated pursuant to the Orders. Sectors of the Russian economy were targeted for restrictions. Three Directives limit US Persons' rights to conduct transactions with sanctioned parties in specified equity and debt instruments of Russian entities. A fourth Directive bans certain transactions relating to Russian oil production.

Generally, US economic sanctions fall into two categories: transactional or blocking. Transactional sanctions prohibit all or specified exportation, re-exportation, sale, or supply, directly or indirectly through a third non-sanctioned country or person, from the US, or by a US Person, wherever located, of any goods, technology, or services to a particular country, foreign nationals thereof or market sector. Blocking sanctions freeze the property and any interests therein of those sanctioned plus anyone that assists, sponsors, or provides financial, material, or technological support for, or goods or services in support of, those targeted that comes into the possession or control of US persons. The term 'interest in property' is defined very broadly to include, among others, indirect or beneficial interests. Entities owned or controlled by, or acting or purporting to act, directly or indirectly, for or on behalf of a blocked person or entity are covered as well.

'US persons' must comply with the sanctions. A 'US person' is any US citizen, permanent resident, entity organised under US laws, including foreign branches, or any person or entity actually in the US. Subsidiaries of US companies organised under foreign law and operating outside the jurisdiction of the US are not generally covered by the sanctions except those relating to Cuba and Iran. However, as noted above, the sanctions have extraterritorial reach to non-US parties if there is even the minimal connection with the US.

One may not do indirectly through a non-sanctioned party or country what one cannot do directly. Engaging in business with an unsanctioned party or country knowing or having reason to know the beneficiary of the activity is a sanctioned party violates US sanctions.

Nor may one facilitate a transaction by a sanctioned party. 'Facilitation' is interpreted by the US government very broadly. Illegal facilitation occurs where a party, presented with a transaction that it cannot complete because US sanctions prohibit it, instead refers the matter to a non-US third party not covered by US sanctions to complete the transaction. The mere referral could serve as a basis for a criminal facilitation charge.

The penalties for sanction violations, as noted above, can be draconian. Forfeiture of the proceeds of offence can be in the millions of dollars, just as criminal fines. Individuals face substantial imprisonment.

Conclusion

As countries turn to economic sanctions to press their international interests the interests of business will collide with them. Given the drive towards economic survival oftentimes unfettered by international law considerations, businesses may look for lawful avenues to circumvent the prohibitions. Knowing where the line is drawn between lawful and culpable lies will be crucial to avoiding bet-your-company penalties.

Note

* **Mark J Biros**, head of Proskauer's Embargo/Sanction International Practice, has handled matters under these laws for nearly 30 years. While with the United States Attorney's Office in the District of Columbia he supervised an undercover programme with US Customs designed to investigate and prosecute violations of the economic sanctions. Working with the Intelligence Community the focus of the operation was military and national security technology and goods plus other goods, services and technology proscribed by the OFAC regulations.
Since entering private practice Mr Biros has represented multinational companies in investigations by the US Department of Justice, OFAC and the Department of Commerce Bureau of Industry Security into alleged violations of the sanctions. He also advises clients on compliance with economic sanctions. His biography is at www.proskauer.com/professionals/mark-biros.

CYBERCRIME SUBCOMMITTEE FEATURES

Cybercrime – criminal offences, competent authorities and organisation and cooperation thereof in the Republic of Serbia

SERBIA

Tamara Janković
Tomislav Šunjka, Serbia
tamara.jankovic@sunjkalawoffice.com

Tijana Živković
Tomislav Šunjka, Serbia
tijana.zivkovic@sunjkalawoffice.com

Introduction

The computer is one of the most important and most revolutionary achievements of technical and technological civilisation. However, despite all the advantages that bring a huge benefit to mankind, the computer quickly became a means of abuse by unconscious individuals, groups and even organisations. Along with the rapid computerisation of society and the entry of the internet into all areas of social and private lives of people, computer crime is becoming the dominant form of abuse, violation of law and norms of behaviour. New forms of attacks on computers and computer networks emerge rapidly, and new types of cybercrime practically depend only on the imagination of malicious perpetrators of criminal offences. Cybercrime may lead to serious damage such as abuse of intellectual property rights, loss of confidential business information, loss of sensitive business information, including possible market manipulation, additional costs of providing network security and recovery from cyber-attacks and reputational damage. Due to all the aforementioned, combating cybercrime has become highly important and includes cooperation with a variety of authorities, as well as cooperation

with non-government organisations and citizens.

Relevant regulations

The Criminal Code ('Official Gazette of the Republic of Serbia', nos 85/2005, 88/2005 – correction, 107/2005 – correction, 72/2009, 111/2009, 121/2012, 104/2013 and 108/2014); the Law on the organisation and competences of government authorities combating cybercrime ('Official Gazette of the Republic of Serbia', nos 61/2005 and 104/2009); the Criminal Procedure Code ('Official Gazette of the Republic of Serbia', nos 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014); the Law on ratification of the Convention on Cybercrime ('Official Gazette of Republic of Serbia', no 19/2009); the Law on International Assistance in Criminal Matters ('Official Gazette of Republic of Serbia', no 20/2009).

Criminal offences

A cybercriminal is a person who commits criminal offences, executing this crime through the use of various tools: computers; computer networks; computer date and their products in material and electronic form. The computer, therefore, becomes an instrument (computer-related crime), or target (computer crime) of a criminal offence. In addition to the aforementioned, there are criminal offences relating to the illegal use of the internet.

Criminal offences against the security of computer data, as defined by the Criminal Code of the Republic of Serbia include: (1) damaging computer data and programs; (2) computer sabotage; (3) creating and introducing computer viruses; (4) computer fraud; (5) unauthorised access to a computer; (6) computer network or electronic data processing; (7) preventing or restricting access to a public computer network; (8) unauthorised use of a computer network; (9) manufacture, procurement, and provision to others of the means of committing criminal offences against the security of computer data.

Besides criminal offences that are listed in the Criminal Code of the Republic of Serbia, the law on the organisation and competences of government authorities combating cybercrime (Official Gazette of the Republic of Serbia No 61/2005 and 104/2009) also regulates this legal matter and, additionally, widens the scope of criminal offences which are deemed to be cybercrime. These are criminal offences against intellectual property, property, economy and legal instruments, where computers, computer systems, data and products thereof appear as the objects or the means of committing a criminal offence. If the number of items of copyrighted works is over 2000, or the amount of the actual damage is over 1m RSD, as well as criminal offences against freedoms and rights of man and citizen, sexual freedoms, public order and constitutional systems and security, these can also be considered, due to the manner in which they are committed or tools used, as cybercrime offences.

The most common forms of cybercrime are related to internet auction sites (e-shop), abuse of credit cards, phishing and identity thefts, 'Nigerian' or '419' scams, and infringements of copyrights.

In the Republic of Serbia, more than half the perpetrators of cybercrimes are young persons under the age of 35. Of these perpetrators, 35.48 per cent have technical and technological knowledge while 24.52 per cent of them have no occupation and 58 per cent are unemployed.

Government authorities

A Cybercrime Unit (the 'Unit') for combating cybercrime has been established within the Ministry of Interior of the Republic of Serbia. The Unit acts upon requests of the Special Prosecutor's Office, in accordance with the law. The minister responsible for internal affairs appoints and dismisses the commanding officer of the Unit, and determines the Unit's activity by following the opinion of the Special Prosecutor. Within the Cybercrime Unit, the Department for Electronic Crime and Department for Combating Crime in the area of Intellectual Property was established as the organisational part for performing duties in regard to more specific areas of fighting cybercrime.

The Higher Prosecutor's Office in Belgrade has jurisdiction for the territory of the Republic of Serbia to proceed in cybercrime matters. The Higher Prosecutor's office established a special cybercrime department – Special Prosecutor's Office. The Special Prosecutor's Office is managed by a Special Prosecutor for the suppression of cybercrime. The Public Prosecutor may request that the courts, other public authorities, local self-government, autonomous province authorities etc, provide him with explanations

and data which may be of use for undertaking actions within his purview.

The Higher Court in Belgrade established a Cybercrime Department which has first-instance jurisdiction in cybercrime matters for the territory of the Republic of Serbia. Judges who act in cybercrime cases are appointed from the judges employed in the Belgrade Higher Court with their consent. Preference is given to those judges who have knowledge in the field of information technology. The trial before the Cybercrime Department is conducted in accordance with the Criminal Procedure Code.

Most important is the cooperation between stated authorities – a public sector with citizens, and legal entities as private sector. Sometimes cooperation is accomplished by direct reporting of criminal offences by the private sector and help with providing the government authorities with relevant information. On the other hand, also of significance is the cooperation of the private sector with organisations such as Net Patrol which is a member of the International Association of Internet Hotlines (INHOPE). Net Patrol, as an internet operator of mechanisms for reporting, offers everyone an opportunity to report illegal and disturbing content through various different reporting methods, and especially child sexual abuse images, sexual exploitation and physical and psychological attacks against children. Net Patrol, after assessment of the report, informs the Unit via email or, in urgent cases, via telephone as well. Additionally, Net Patrol informs the sender of the report that it has informed the Unit. Upon notification to the relevant Cybercrime Unit of the Ministry of Interior, the police shall, within their remit, investigate the case and file criminal charges to the Republic Public Prosecutor's Office in compliance with the law.

The Law on International Assistance in Criminal Matters prescribes mutual assistance between countries regarding: the extradition of defendants or convicted persons; the assumption and transfer of criminal prosecution; the execution of criminal judgments; other forms of mutual assistance.

Conclusion

Due to the newly adopted regulations and widening scope of criminal offences which are deemed to be cybercrime and which fall under the jurisdiction of the Unit, Special Prosecutors Office for High-Tech Crime and a Cybercrime Department established within the Higher Court in Belgrade, the authors believe that the public has developed a consciousness of the high importance of cybercrime protection. Nevertheless, the knowledge about the various forms and means of cybercriminal can be always higher among the Private Sector which is the main victim of cybercrimes perpetrators. Therefore, prevention through education should be one of the most important means of combating cybercrime. When the prevention becomes less effective, especially due to the reason that cybercrime perpetrators change the manner of execution of criminal offences on a day-to-day level, the government authorities shall use their legal authorisation to detect, prosecute and try for cybercrime.

UNITED KINGDOM

Why not use the tools you already have to protect your business against cybercrime?

John Bechelet
Bivonas Law, London
jbechelet@bivonas.com

Rebecca Dix
Bivonas Law, London
rdix@bivonas.com

In a global study conducted by the UN Office of Drugs and Crime in 2013, it was found that up to 17 per cent of reported crimes are classed as 'cybercrime'. In December 2014, 3.1 billion people, 45 per cent of the world's population, had access to the internet and it is estimated that by the year 2020, the number of internet connected devices will outnumber people by six to one. It is therefore not surprising that global law enforcement is struggling to cope with the rapidly growing scale of criminal investigation into online crime.

In the United Kingdom, the imbalance between lack of specialist law enforcement resources and the capabilities of highly skilled and well funded organised e-crime syndicates is coming to a head.

The UK has 800 specialist internet crime police officers, but with estimates of over 30,000 incidents of cybercrime a day it is clear that investigative resources fall woefully short of that required.

A global cost of US$400bn is attributed to cybercrime annually and it is easy to understand why private sector businesses are frustrated by the low number of cyber criminals being brought to justice.

In response, it is anticipated that UK businesses affected by cybercrime will decide to take matters into their own hands by seeking redress through both the civil and criminal courts that will also see a significant increase in the number of private criminal prosecutions.

In England and Wales, any individual has the right to bring a private criminal prosecution. This important common law power is enshrined in statute at section 6 of the Prosecution of Offences Act 1985. Lord Mance observed in *Jones v Whalley* [2006] UKHL 41, that criminal prosecutions: 'may be initiated by private bodies such as high street stores, by charities such as the NSPCC and RSPCA, or by private individuals'.

There is an established pedigree for private criminal prosecutions in areas such as copyright theft. For example, the British Recorded Music Industry (the 'BPI') frequently brings private prosecutions for offences under section 107 Copyright, Design and Patents Act 1988, as do the Federation against Copyright Theft (FACT).

A relatively recent example is a prosecution by Virgin Media which brought criminal proceedings against three men who took part in a large-scale fraud selling set-top boxes which allowed people unlawful free access to Virgin Media's cable subscription service. It was estimated that Virgin's lost revenue as a result of this fraud was £380m. The private prosecution resulted in convictions for all three men.

In order to privately prosecute it is necessary to first identify the offence which has been committed. The term 'cybercrime' is broad and rather amorphous; cybercrime offences can be most conveniently divided into two categories:

- cyber-dependant crimes; and
- cyber-enabled crimes.

First, cyber-dependant crimes are offences that can only be committed using a computer, computer networks or any other internet connected device. These acts include hacking, the spread of viruses and malware or distributed denial of service (DDoS) attacks, and generally fall under the scope of the four offences set out in the Computer Misuse Act (CMA) 1990, as follows:

- section 1 – unauthorised access to computers;
- section 2 – unauthorised access to computers with the intent to commit or facilitate further offences;
- section 3 – unauthorised acts with the intent to impair, or being reckless as to the impairment of, a computer; and
- section 3A – making, supplying or obtaining articles for use in offences under section 1–3.

A cyber-enabled crime is a 'traditional' crime which has been facilitated by the use of computers, computer networks or any other internet connected device. Broadly speaking, the majority of cyber-enabled crimes fall

under two traditional types of offence: fraud or theft. Whilst conceptions of the internet and all things cyber rapidly change in this new, hyper-connected world it will soon become hard to imagine a financial or business crime that is not cyber-enabled.

The most widely publicised and often most financially damaging incidences of cybercrime is fraud, and offences of this nature will generally be prosecuted under the provisions of the Fraud Act 2006. Cyber-enabled fraud can take various forms, including:

- electronic financial frauds, most notably online banking frauds and internet-enabled card-not-present (CNP) fraud;
- mass-marketing frauds and consumer scams, including phishing scams which use disguised fraudulent emails as legitimate email communications and ask for personal or corporate information from users such as passwords or bank account details; and
- 'pharming' where an internet user is directed to a fake website and then prompted to input personal details or financial data.

Personal data theft is also a common offence which is facilitated by the use of computers and the internet.

There are a number of offences that are created from the misuse of computer data, for example, section 55 Data Protection Act (DPA) 1998 which prohibits knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller; section 1 Malicious Communications Act 1998, which makes it an offence to send indecent or grossly offensive electronic communications with the intent of causing distress or anxiety, and section 127 of the Communications Act 2000 which criminalised the improper use of internet communications, a statute which is now regularly used to prosecute internet 'trolls'.

Before commencing proceedings a private prosecutor must first undertake the investigation stage, in the same way that the police are required to investigate a crime. Much of this investigation can be carried out in-house; however it is likely that police assistance will be required as a private individual may not have the power of arrest, to obtain search warrants or the power to conduct a financial investigation into any suspect.

Following the investigation stage, the procedure for commencing a private prosecution is set out in part 7 of the Criminal Procedure (Amendment) Rules 2015 (CPR).

Once all necessary evidence has been gathered, the prosecutor must lay any information before the magistrates' court in order that a summons can be issued. CPR 7.3 prescribes the format which the Information must take:

(1) an allegation of an offence in an information or charge must contain:
  (a) a statement of the offence that -
    (i) describes the offence in ordinary language, and
    (ii) identifies any legislation that creates it; and
  (b) such particulars of the conduct constituting the commission of the offence as to make clear what the prosecutor alleges against the defendant.
(2) more than one incident of the commission of the offence may be included in the allegation if those incidents taken together amount to a course of conduct having regard to the time, place or purpose of commission.

When reaching its decision as to whether or not to issue a summons, the magistrates' court will consider the following factors:

- whether the offence is known to law and the elements are present on a prima facie basis;
- whether the court has jurisdiction;
- whether the informant has authority to prosecute (that the permission of the Director of Public Prosecutions (DPP)) has been obtained where the offence in question so requires);
- whether a limitation period applies; and
- whether the allegation is vexatious.

It is important, therefore that the prosecutor also considered these factors in advance of applying to the magistrates' court.

Once the summons has been issued a private prosecutor may wish to apply for the restraint order over the defendant's assets, in order to secure realisable assets to make them available for any confiscation order made on conviction, pursuant to section 40 of Proceeds of Crime Act (POCA) 2002.

Thereafter a private prosecution will follow the same path as a case brought by a public prosecuting authority. The prosecution will be required to put forward its case, and the defendant is afforded the opportunity to put forward a defence.

Unless specified in statute the Magistrate will decide whether the case will be tried in the magistrates' court of before a jury in the crown court, and this will be determined by the seriousness and complexity of the offence. Summary offences, such as section 3 offences

under the CMA 1990, will be heard at the magistrates' court; whilst indictable offences, for instance a serious fraud, will be heard at the crown court. If the defendant is convicted then the court will impose the appropriate sentence against the defendant, which may include a payment of costs to the prosecutor.

Following a successful conviction, it is possible for a private prosecutor to pursue any confiscation proceedings against the defendant under POCA 2002.

In the *Virgin Media* case referred to above, the court made a confiscation order in the sum of £11.8m and Virgin Media was subsequently awarded its costs for the proceedings from central funds, pursuant to section 17 Prosecution of Offences Act 1985.

It is now well established that the costs for a private prosecution in the crown court may be payable from central funds. A wealthy Indian businessman, Murli Mirchandani, who was the victim of fraud recently recovered his costs of just over £400,000 from central funds and secured a jail term of eight years for the perpetrator.

There are a number of reasons why an organisation may wish to instigate a private prosecution; to prevent a competitor from unlawfully profiting from criminal conduct or to act as a deterrent to further offending in order to protect a business; for example employee hacking or data breaches. Whatever the reason private criminal prosecutions are a powerful old tool that is still readily available to use in tackling the ever increasing commission of cybercrime.

UNITED STATES

Frederick T Davis
Debevoise & Plimpton LLP, Paris
ftdavis@debevoise.com

A US prosecutor's access to data stored abroad – are there limits?

On 9 September 2015, the United States Court of Appeals for the Second Circuit will hear argument on an appeal by Microsoft from an order by the District Court in the Southern District of New York compelling Microsoft to turn over to the United States Attorney emails and related data relating to an unidentified customer of Microsoft ('John Doe') who is the target of a criminal investigation. Microsoft resisted this order on the ground that the data in question was located outside the United States. Specifically, it argued that John Doe had identified himself as a citizen of Ireland when he opened his account; that under its normal policy Microsoft keeps almost all data (including the content of any emails sent or received) of its customers on the server closest to the place of residence in order to minimise delays associated with 'latency'; that the relevant data relating to John Doe was thus stored on a server in Ireland; and that Microsoft disclaimed the legal obligation to obtain for the US Attorney data stored on its server in Ireland, although it had the technical ability to do so. A magistrate judge ordered Microsoft to provide the information, and this decision was affirmed by a judge of the District Court. Microsoft's appeal has been supported by an unusually large number of 'friend of the court' briefs filed by entities with an interest in the subject, including the Republic of Ireland, a Member of the European Parliament , a number of service providers (such as Apple, Verizon, Accenture and many others), and constitutional law groups.

This article will focus on a question that may or may not be addressed by the Court of Appeals, but which will in any event have a significant bearing on how its decision may be received outside the United States. Does the District Court's order comply with principles of international law, and in particular principles relating to the appropriate limits of a country's exercise of legislative, judicial or police power when that exercise may have an impact on another country's interests? This is important because a decision widely understood as contravening international law – particularly if it is viewed as not respecting

principles that other countries would respect if the issue were to arise there – could lead to negative consequences, such as decreased cooperation in transnational criminal matters, or retaliation against US law enforcement authorities or service providers.

Because of this focus, there are a number of issues vigorously discussed in the parties' submissions and by the *amici curiae* that will not be addressed here, even though they are important and could be dispositive of the appeal. The two principal issues not addressed here are:

- *The proper interpretation of the Stored Communications Act (SCA)*
  The SCA was adopted by the US Congress in the mid 1980s, before email became the dominant and ubiquitous form of communication that it is today. Many of the arguments made to the magistrate judge and the District Court concerned its proper interpretation. This article will assume that, however the Court of Appeals decides issues under the SCA, that decision will nonetheless be viewed in the context of its appropriateness under international law.
- *The Constitution of the United States*
  Some of the friends of the court urge that protections provided in the US Constitution, notably the Fourth Amendment's limitations on official 'search and seizures,' bear on the Court's analysis. Again, this article offers no opinion on this question, but simply assumes that, however the Court deals with domestic constitutional issues, the result should also be analysed from an international legal perspective.

This article also assumes the procedural regularity of the prosecutorial process – that is, that the prosecutor had a sufficient basis to seek the information held by Microsoft, and followed appropriate criminal procedures in doing so.

The facts and procedural history

Both the relevant facts and the procedural history are relatively simple.

As noted, John Doe is being investigated by the federal prosecutor in New York for possible violations of federal criminal laws. In the course of this investigation, the investigators learned that John Doe maintained an email account pursuant to a service offered by Microsoft. In search of evidence or leads relevant to the investigation, the prosecutor decided to obtain copies of John Doe's account information, including emails sent and received by him. Obtaining information from third parties about a person under investigation is of course a standard investigative procedure; requests to service providers for this purpose are made constantly.[1]

In the John Doe case, and pursuant to SCA procedures described in a bit more detail below, the prosecutor applied to a federal judge for, and was granted, a 'warrant' that directed Microsoft to produce to the prosecutor (without alerting John Doe) copies of all emails stored in his account, all information relating to his identity (such as the name and addresses provided), and any other information stored therein (such as names and addresses of correspondents). As a frequent recipient of such official demands, Microsoft maintains a 'criminal compliance office' tasked with responding to them; this office has the technical capacity to find and retrieve data maintained by its customers, even if the data is maintained outside the United States.[2] The compliance office determined that John Doe had identified himself as a resident of Ireland, and that consistent with standard Microsoft policy, and to minimise performance delays caused by 'latency' in the event of increased distance between user and server,[3] John Doe's account was 'hosted' on a server maintained by Microsoft in Dublin, Ireland. As a result, all but a very small amount of the data sought by the government's warrant did not exist on any US server, but could only be found in Ireland. The small amount of data maintained in the US consisted of information sufficient to identify the John Doe account and point to its location in Ireland, as well as a small amount of 'quality control' information, but apparently did not contain any 'content' of investigative use to the prosecutor.[4]

Upon learning of the location of the data, Microsoft informed the government that it would provide the (essentially useless) US-based information but that it would not provide information from its Irish server, even though it had the technical ability to obtain that information by taking simple steps in the US, apparently without undue cost or difficulty. Upon the refusal of the prosecutor to accept this, Microsoft filed a motion to 'quash' the warrant on the basis that it was not authorised by the SCA and that it called for an extraterritorial application of US laws that was neither intended nor appropriate. The magistrate judge denied

this application in a 26-page written opinion. His decision was reviewed by a judge on the District Court, who affirmed it.[5]

The Court's decision

The relevant SCA provisions

Much of the magistrate judge's opinion explored the SCA procedures for the prosecutor to obtain the John Doe data. The Court noted that the SCA was an attempt by the US Congress to provide mechanisms to balance the largely opposing needs of, on the one hand, governmental access to information in criminal and other contexts, and, on the other hand, the privacy rights of individuals. Since the SCA was adopted at a time when 'data storage' was in a relative infancy, it speaks in general terms and does not, for example, single out emails for specific treatment. It nonetheless provides a straightforward approach to the basic circumstance presented in the John Doe case by offering the prosecutor three different procedures to obtain personal information, each with a different burden of proof and judicial oversight depending on the intrusiveness of the inquiry.

The simplest procedure is for the prosecutor to issue an 'administrative subpoena', which the prosecutor can easily do in the name of the grand jury, which compels the information holder (such as Microsoft) to produce designated information. The prosecutor can issue such a subpoena without any judicial intervention, and without any specific demonstration of need.[6] However, under the SCA the subpoena approach has some very important limitations:

- it permits the prosecutor only to obtain basic customer information, unopened emails more than 180 days old, and opened emails;[7]
- the prosecutor must give notice to the customer, although notice may be delayed for up to 90 days upon the written certification of a supervisory official; and
- if the prosecutor delays giving notice, they may request a court order barring the ISP from notifying the customer for a like period.

The prosecutor can alternatively ask a judge to issue a 'court order,' which permits access to further information in addition to that available under a subpoena, including a history of all emails sent or received by the customer (although not their content). The 'court order' procedure differs from the issuance of a subpoena in certain respects:

- the prosecutor cannot issue it unilaterally, but must demonstrate to a judge 'specific and articulable facts showing that there are reasonable grounds to believe' that the information sought will be 'relevant and material to an ongoing criminal investigation'; and
- the prosecutor must provide notice to the affected party. Such notice cannot be delayed unilaterally, but can be delayed by court order and the judge can again bar the internet service provider (the 'ISP') from notifying the client/subscriber for a like period.

Finally, the SCA permits the prosecutor to ask a judge to issue a 'warrant,' which permits the prosecutor to obtain, in addition to information obtainable under a court order, unopened emails stored for less than 180 days, without informing the account holder. Under the Federal Rules of Criminal Procedure, a judge can issue a warrant only upon a showing by the prosecutor of 'probable cause' to believe that the information sought will provide 'evidence of a crime' or the fruits thereof – a somewhat higher standard than the 'reasonable grounds' necessary to obtain a court order.[8] The SCA does not require notice to the customer for the execution of such warrants.

None of the SCA provisions summarised here specifically addresses their intended extraterritorial reach – that is, whether they should or should not apply when responsive information is located outside the United States.

The Court's reasoning

Microsoft's principal argument was appropriately described by the magistrate judge as 'simple, perhaps deceptively so'.[9] It argued that under accepted jurisprudence, a 'warrant' issued under Rule 41 of the Federal Rules of Criminal Procedure is limited to the territory of the United States and cannot be exercised outside of it; thus, it argued, the warrant issued here could not be executed upon data found in Ireland. Magistrate Judge Francis rejected this argument. His principal bases for doing so were as follows.

- First, he noted that the traditional basis for restricting the execution of a warrant to US territory is that historically a 'warrant' authorises a law enforcement officer to enter a physical place (such as a home or

place of business), and that it would – in that context – be clearly inappropriate for such an officer to do so outside the United States. Here, he reasoned, no official investigative activity would take place outside the US at all, since the warrant called for Microsoft to obtain, and then produce, the requested information without anything happening outside the United States.

- Secondly, he noted that both subpoenae and court orders applicable to lesser intrusions as noted above were not, historically, limited to information located in the United States. It has long been the law, for example, that a person or corporation located in the US must respond to a subpoena calling for information located outside the US if it 'controls' that information, in the sense of being able legally and physically to access and produce it.[10] Reasoning that the 'warrant' was in fact a 'hybrid' structure, the Court concluded that there is no reason to believe that the Congress intended one approach to the extraterritorial reach for subpoenas and court orders, but a much more restricted one for warrants.

In a short concluding section of its opinion entitled 'Principles of Extraterritoriality,' the magistrate judge reasoned that concerns relating to application of US laws outside the country's borders 'are simply not present here'.[11] He noted that the *Morrison*[12] and *Kiobel*[13] decisions of the Supreme Court create a strong presumption that US legislation applies only within the country's borders, absent a showing of legislative intent otherwise, and implicitly acknowledged that nothing in the SCA specifically evidenced an intent that it should apply outside US borders. He nonetheless concluded that *Morrison* and *Kiobel* do not apply because Microsoft was located in the United States and would comply with the warrant without leaving the United States or committing any act outside of it: the warrant 'places obligations only on the service provider [that is, Microsoft] to act within the United States.' The Court ended its discussion of extraterritoriality noting that:

> '[A]n SCA warrant does not criminalise conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored.'[14]

Discussion

Legal principles relating to extraterritoriality.

The Microsoft appeal implicates classic principles of international law defining the limits of the territorial reach of a country's laws and their execution, and requires their application to relatively recent – and increasingly important – technological and commercial realities that were not fully understood when the prevailing rules relating to extraterritoriality were developed.[15] As will be discussed below, rules relating to 'sovereignty' emerged from contexts implying a close and intuitively obvious link between the activity to be regulated and the actual place (or 'territory') involved. When applied to data held in the 'cloud' and frequently stored on servers physically located in locations distant from activity that one country may wish to regulate, classic rules of international law may be difficult to apply, and require sophisticated analysis of the principles at stake.

The limits of a state's right to project its laws or powers 'extraterritorially' are sometimes viewed as having three components:

- the 'power to prescribe,' that is, the power to adopt laws affecting conduct;
- the 'power to adjudicate,' consisting of the power of a country's courts to issue valid decisions relating to the questions and persons before it; and
- the 'power to execute,' which refers to the power to enforce laws or judgments.[16]

All three may be implicated by the Microsoft matter – the case addresses:

- the power of Congress to apply provisions of the SCA (and of US criminal laws generally) outside the territory of the US;
- the adjudicatory power of US courts (among other things, to issue 'warrants' or 'court orders' that may have impacts beyond US borders); and
- the power of enforcement agencies to enforce the SCA, the warrants issued by US courts, and other mechanisms that may be involved in official pursuit of data stored outside the US.

In a general but very important sense, all three components rest on two common concepts: that application of one country's laws outside of its territory must be based on a reasonable and valid state interest; and secondarily that its interpretation and

execution must be take into account the reasonable and valid interests of other states. The jurisprudence developing these principles has focused on two principal conclusions:

- every state is considered to have the power to address conduct that takes place on its *territory*, whether done by a citizen or not; and[17]
- every state is considered to have the power to address the conduct of its *citizens*, whether or not that conduct takes place on its territory.[18]

While simple in theory, both principles have evolved in ways that raise particular questions in the context of the Microsoft appeal.

The principle of territoriality has been expanded by the so-called 'effects' test. This approach expands the valid exercise of state power beyond addressing acts *committed* on its territory to include acts the effects of which (even if committed overseas) are *felt* on a state's territory. The classic example of this analysis is a cartel where the participants may enter into, and execute, an agreement to fix prices without ever setting foot in a country that nonetheless would suffer the economic consequences of an illegal agreement.[19] The 'effects test' was developed in US jurisprudence to investigate and prosecute overseas cartels, and was approached warily by countries in Europe; more recently courts and administrative agencies in the European Union have generally adopted the concept.[20]

While external application of national laws on the basis of citizenship raise few questions when applied to natural persons, it becomes increasingly complicated when applied to corporations (and other synthetic 'persons'), since the 'citizenship' (generally understood to be the place of incorporation, or of the principal place of business) of a company can be adjusted almost at whim by its owners through myriad means of incorporation of parents and subsidiaries, and other corporate relationships.

Technical and commercial developments that affect the analysis

Changes in technology over the last generation have, self-evidently, been vast; and they will surely continue into the future. One general phenomenon bears emphasis here, which may be called the element of 'deterritorialisation' or 'delocalisation.' Traditionally, laws and traditions protecting privacy have focused on principles linked to a physical place or *territory*. The Fourth Amendment to the US Constitution, for example, refers to 'the right of the people to be secure in their persons, houses, papers, and effects…'. The reference in the same Amendment to the requirement of a 'warrant' as a prerequisite to seizing a person or thing, and the insistence that it not be issued other than upon 'probable cause,' had a clear territorial, or physical, reference: whether to detain a 'person,' enter a 'home,' or seize a 'paper' or 'effect' – all required physical access to a specific place. It is thus clear why, traditionally and as set forth in Rule 41 of the Federal Rules of Criminal Procedure, a 'warrant' could not have any effectiveness outside of the territory of the US – precisely because a warrant permitted a state actor (such as the police) to act in a physical place (the location of a person or a thing), its execution could not occur outside of the territory of the US without infringing on the sovereign rights of another country.[21]

In the 18th century and well into the 20th, information was stored in 'papers', very much linked to the 'place' where papers were stored. The early phases of 'the computer revolution' and the storage of information as digitised data did not cause a huge change in this traditional frame of reference, because data was initially stored on fixed media such as floppy disks and hard drives; those media – much like 'papers' – had a physical location, and it did not cause too much difficulty to adapt Fourth Amendment jurisprudence, and rules relating to searches and seizures, to them.

The explosion of cheap and high-speed data transmission together with radically reduced costs of storage changes this. As one writer recently observed, 'the infrastructure of the internet means that data are not territorially bound.'[22] While people continue to store data on local hard drives and memory sticks, increasingly data is stored at the very least on a 'network' of linked computers and often in 'the Cloud'. The Cloud, in turn, may consist of any number of different phenomena, sometimes in tandem, including the following:

- Data may be stored on a server that is extremely remote from the persons storing (and later getting access to) the data; this may include storage in a completely different country.
- Because of the low cost of data storage and the need for security, there are often automatic backups so that the same data

appears simultaneously in more than one place.[23]
- At least with respect to data in transit, a 'document' or other piece of information may be broken into 'packets' of data and routed separately to a destination where they are reassembled.[24]
- Casual users of the Cloud may not know or care where their data is stored, but someone concerned about anonymity can deliberately choose a remote location where third-party access is restricted by local law or custom.
- While encrypting physical documents is difficult and expensive, encrypting digitised data is not.

Still further disassociation of data from territory may be possible. Some data storage companies have already spoken of creating 'data farms' on the high seas where at least in theory the physical location of the data is not subject to any country's jurisdiction;[25] it is even possible to imagine storing data on satellites in space.

Separately, technology offers a different threat to law enforcement authorities if data storage companies adopt and make available to their customers the fruits of so-called 'public-key cryptography' technology: Data companies could easily advertise that their customers can choose an encryption system where the 'key' to reopen encrypted communications is retained by the customer alone.[26] Under this scenario an ISP confronted with a warrant could hand over encrypted data, but neither the ISP nor the investigator could decrypt it. This would permit encryption that under current technology cannot be broken (or at least cannot be broken without an undue expenditure of time of time or resources), and thus access by a State to information stored by a customer could not be had from the storage provider at all, irrespective of the legal procedure followed or the demonstration of need.

The parties' interests

Analysis of international law principles depends in part on weighing the respective interests of participants. The participants whose interests will be reviewed are:
- the 'Requesting Country' (the US, speaking through the federal prosecutor);
- the 'Host Country,' Ireland, where the relevant data is stored;
- the 'Owner' of the data, John Doe; and
- the 'Internet Service Provider' or 'ISP,' Microsoft.

The requesting Country

The obvious and legitimate interest of the prosecutor is to obtain information in aid of his or her investigation. It is essentially irrelevant to the prosecutor where that information is stored. Thus, the interest of the prosecutor is no less and no more legitimate with respect to data stored overseas than with respect to information traditionally obtained through 'search and seizure' procedures domestically. The US does have a secondary interest in maintaining good diplomatic relations with other countries from which it may seek cooperative help in criminal investigations, and thus in observing international rules since rejecting them may diminish cooperation.

The interest of the host country

While Ireland submitted a brief as *amicus curiae*, it did not specifically take a position on how the Court of Appeals should rule; nor did it explicitly state its interest in the matter. (Its principal purpose was to express its willingness to fulfill all its obligations under its Mutual Legal Assistance Treaty with the US, and to bring to the Court's attention a recent decision of the Supreme Court of Ireland relating to access to bank data held abroad). Evaluating the inherent interests of any country hosting data that may be sought by US procedures is nonetheless critical to a reasoned analysis.

The record is incomplete with respect to two issues of possible relevance. First, it is unclear the extent to which John Doe is, in fact, a citizen or resident of Ireland; while he indicated on applying for a Microsoft account that he resided there, this was not verified. Secondly, and more broadly, it is unclear whether John Doe's activities under investigation had any link to Irish territory, apart from the claimed residence of the owner and the fact that Microsoft chose to store his email data there.

Depending on these two variables, one could construct hypothetical situations where the host country's interests could be quite different:
- It is possible that Mr Doe is not only an Irish citizen but that all of his activities relevant to the US investigation took place in Ireland.

- Alternatively, it is also possible that he is a US and not an Irish citizen; that he has never even been in Ireland; that all his potentially criminal acts (including email correspondence) took place in the United States; and that his email data are stored in Ireland only because he lied in providing account opening information to Microsoft.

In the first hypothetical, Ireland would appear to have a genuine interest in protecting the privacy of one of its citizens. In the second, it is more difficult to determine Ireland's real interest.

Viewed generally, a host country may have interests in data stored on its territory, irrespective of the question of citizenship or territory-based activity:

- First, a host country may have an economic interest in encouraging 'data farms' on its territory, which could be expected to bring some revenue, and would worry that its reputation for such activities would be adversely affected by perceptions that data stored there can be accessed from outside the country.
- Secondly, it may have a general, but important, concern about its 'sovereignty', and resent a ruling by a US court that any company that stores its data in Ireland can be forced to turn over that data to US prosecutors without going through formal diplomatic channels, and thus that data stored in Ireland can be produced overseas without Ireland even knowing.

The terms of some mutual legal assistance treaties and legislation relating to international data transfer provide insight into the sovereign interest of a country in data stored on its territory.

A number of countries have adopted so-called 'blocking statutes,' the purpose of which is to prohibit the transfer of information outside of the country without going through international conventions or agreements that, at a minimum, provide authorities in the host country with notice of any request for information and the opportunity to exercise control over the release of such data outside of its territory.[27] Under the Court's existing ruling in the *Microsoft* case, no host country would even have a right to be informed if a company storing data on their territory were obligated to turn such data over to a US prosecutor, thus eviscerating the effect of national legislation such as the 'blocking' statutes.

A number of international treaties clearly contemplate some degree of supervision or control by a host country over access to data stored there. For example, Article 9(2a) of the Agreement on Mutual Legal Assistance (the 'Agreement') between the EU and the US, signed in 2003, provides that the host country (or, as used in the Agreement, the 'requested country') to whom a request for mutual assistance is made may add certain 'limitations' on information transferred 'to protect personal and other data.' An 'explanatory note' to this Article makes it clear that the host country must be in a position to make a case-by-case determination of the need for such protection in order to avoid an overbroad or inflexible rule:

> '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, 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 specialized 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).'

This provision – found in an important treaty between the US and Europe relating to mutual legal assistance in criminal matters – clearly shows that both the US and the countries in the EU think that they have a say about whether to allow the transfer of data out of their respective countries. This interest would necessarily be undermined by the current ruling in the *Microsoft* case, since it would permit the transfer of data out of Ireland without Ireland even being aware of the request or the transfer.

The owner

John Doe obviously has a personal interest in resisting disclosure of his personal information, a right that may be expressed as his right to 'privacy' but also to procedural regularity with respect to a criminal investigation of him. Since the right to privacy is not absolute, his legitimate interest is whether proper procedures were followed to permit the prosecutor to obtain his personal information.

From all that appears in the record, it seems that John Doe has no basis under US law to contest the adequacy of the procedures used to obtain his information. Under the SCA and Rule 41 of the Federal Rules of Criminal Procedure, the prosecutor must have demonstrated to the satisfaction of a neutral judge that there was 'probable cause' to conclude that John Doe was responsible for a federal crime, and that evidence in his email account would shed light on this. The public record does not disclose what that showing of probable cause was; for present purposes the only appropriate presumption is one of regularity, that is, that a sufficient showing was made. While that showing was not one to which John Doe had the opportunity to oppose, under US procedures he would get that opportunity if he is indicted and the fruits of an email search were offered against him.

On the present record, it is difficult to see how Mr Doe could argue that Irish rather than US standards should be used to evaluate whether he has been treated fairly. If John Doe was a legitimate target of a US criminal prosecution – that is, if the US was 'competent' to proceed against him – he would have no basis to argue that because of his Irish citizenship or other non-US contacts he was protected by non-US rules. Otherwise put, there is no international principle that suggests that prosecutors have to follow different rules when the target of their investigation is not a US citizen.[28]

The Internet Service Provider

The real interest of the ISP, in this case Microsoft, appears to be primarily commercial. While Microsoft has vigorously pursued this appeal emphasising the procedural restraints on governmental authority necessary to protect the privacy rights of its customers[29] – a theme also emphasised in the many friend of the court briefs filed by other commercial enterprises – the only basis for a non-vicarious (or non-altruistic) interest is the perceived risk of a competitive disadvantage if it is ordered to turn over John Doe's Irish data. As the trial judge noted in his opinion, Microsoft is a large American company with the acknowledged technical ability to easily obtain the data that it elects to store overseas. Microsoft (and similarly situated US companies that appear as *amici*) are clearly concerned that an adverse ruling will be interpreted by potential customers to mean their data is not safe with an American service provider who can easily be forced to share data with the prosecutor, irrespective of the location of those data. A broadly worded adverse ruling could also damage their business by leading to scenarios where a US court might hold them in contempt if they do not produce the requested data, but the production of that data is a punishable offence in the nation where the data is hosted.

The parties' legal positions

The outcomes proposed by the federal prosecutor and by Microsoft could not be more diametrically opposed.

The position of the US government

The prosecutor argues that the issue is very simple because the courts have already ruled that any entity that is 'present' in the US (or that is subject to its personal jurisdiction) can be ordered to produce any data that it 'controls', irrespective of the location of that data. This position was essentially adopted by the District Court. It raises a few questions.

While much of the discussion about the case has focused on the obvious fact that Microsoft is a large, and indeed iconic, American enterprise, the government's position, if adopted, would not be limited to US companies. Rather, it would apply to *any* company over which the prosecutor can convince a court that it has power to enter a binding and enforceable order – that is, as to which the courts can exercise the 'power to adjudicate' (see above). While the breadth of this ruling might assuage somewhat a concern that US companies would be singled out and thus suffer a competitive disadvantage, it may be difficult for non-US companies to determine whether their activities in the US in fact subject them to American personal jurisdiction, and some may be legitimately surprised by the exercise of US 'long arm' jurisdiction over them.

It is, in fact, often difficult to determine the extent to which courts may exercise 'personal jurisdiction' over parties based upon their activity on the internet.[30]

The position of the US government is particularly troublesome because it fails to recognise any legitimate interest at all of the countries where the data it seeks may be found. In taking this position, the prosecutor echoes the conclusion of the District Court, quoted above, that the Court's order does not raise 'extraterritorial concerns' because it does not compel any activity to take place on foreign soil. This reasoning, however, does not take into account the *effects* of the Court's order, which definitely would be felt on foreign soil to the extent that data found exclusively on it is produced in the US, because it would deprive the host country of the ability to make a determination – expressly permitted by the US/EU Treaty, for example, – whether a requested transfer violated its privacy or other laws. As noted, a purely 'territorial' analysis has already evolved to consider the interest of the country where effects are felt, and not just those where the acts took place (see above). While invoked as a basis to justify expanded US authority to rule on activity taking place outside of the territory of the US, it would logically imply that an appropriate exercise of that authority should consider the effects of US-based activity that are felt elsewhere. In a different context, when high-tech criminals located outside the US target US victims by 'hacking' or other means, they do so without in any way taking acts inside the US, but it is intuitively obvious that their acts implicate US sovereignty (and thus the right of the US to regulate or prosecute) because of the 'effects' of their acts.

The position of Microsoft

Microsoft's position, supported by many *amici curiae*, is that the only means by which a US prosecutor should be able to obtain data stored abroad is through an international treaty, bilateral agreement, or other state-to-state mechanism. In so arguing, Microsoft appears to take for granted the interest of the host country. The rule it proposes, however, is both overbroad and inflexible and thus treats in the same way situations that may be quite different. One could imagine a situation involving the following hypothetical elements:

- an individual we will name James Doe is a US citizen who is part of an organised US-based criminal gang. Aware that emails, while useful to his nefarious plans, may be recovered through investigative means, James selects a non-US ISP known to be based in, and to store its data in, the territory of a country that has no MLAT or similar agreement with the US, and with which the US has bad diplomatic relations. In filling out his account opening form, Mr Doe lies and says that he is a citizen of the country hosting the service.
- Without once leaving the US, Mr Doe constantly uses his email to reach out to fellow gang members, and also uses it to defraud victims – in short, his email use in the US generates very compelling proof of his crimes. But he carefully 'wipes' his computers, so that the only place where the content of these communications can be found is on the server in the hostile country.

Under Microsoft's analysis, it would appear that the prosecutor would be almost powerless to obtain these data, and would be reduced to applying diplomatic pressure to negotiate with the hostile foreign state.

An approach that conforms with international legal principles

Any ruling by the Court of Appeals will risk mischief if it attempts a simple 'one rule fits all' outcome, including either of those proposed by the parties. While there is an obvious need for administrative simplicity, the following procedures would not overburden the wheels of justice; and they are far more likely to yield results that would be viewed outside the US as consistent with international law – and thus would not cause any risk of retaliation.

- If a prosecutor or other governmental authority seeks information stored as data, it can proceed using any of the SCA procedures according to the circumstances.
- An ISP receiving a subpoena, court order or warrant may resist compliance on the grounds that the data sought is located exclusively outside the US only upon a showing that:
  - there is an objective basis to believe that the Host Country may have an actual and valid interest in the data stored there, which may entail a showing that:
    - † the account holder is a verified citizen or resident of that country; *and/or*

  - † that the use of the account has been predominantly in the host country; *and*
  - the host country in question has a demonstrably acceptable record working cooperatively with the US through MLATs, international treaties, or other arrangements.
- The prosecutor can rebut this by showing that:
  - there is objective basis to believe that the account holder actively used the account as part of a criminal act and while in the US; *or*
  - there is an objective basis to believe that, while outside the US, the account holder actively used the account as part of a criminal act that was intended to, and foreseeably will, have a material effect in the US; *or*
  - the host country in fact is not cooperating effectively with the US; *or*
  - there is a special emergency where recourse to bilateral cooperation would be ineffective.

Overlapping territorial jurisdictions, or concurrent jurisdiction, is not a new concept. The paradigm example from the infamous *SS Lotus* case of two ships, flying the flags of different nations, colliding in international waters, shows that such occurrences were possible, even without modern data processing and storage techniques. In that case, both France and Turkey had territorial jurisdiction over their own ships, as extensions of their respective territories, and so either country could have adjudicated the dispute. Analogously, just because the US has territorial jurisdiction over Microsoft within its territory, does not deprive Ireland of jurisdiction over data found on its servers. However, where ships colliding was a relatively rare occurrence, modern data storage techniques will frequently implicate concurrent jurisdiction as companies make use of remote data processing sites. A legal framework which accounts for modern data storage practices must do more than inquire into whether a state has the power to compel data disclosure. Any successful long-term solution must meet the requirements of comity by balancing the legitimate interests of the countries that may be affected by the exercise of that power. The approach presented here allows for efficient service of non-controversial SCA 'warrants', while providing a mechanism for ISPs like Microsoft to show that, in a particular case, there is a treaty process that is the more appropriate procedural device because of the apparent legitimate interest of the host country and its history of compliance with applicable cooperation treaties. Whatever solution is eventually adopted in the Second Circuit will be judged by the rest of the world on how well it conforms to comity and the principles of international law.

Notes

1 While agencies do not report the number of subpoenas they issue per year, the figure is thought to be huge. An example reported in *Wired* is that AT&T responded to 131,400 subpoenas for customer information in the year 2011 alone: David Kravits, 'We Don't Need No Stinking Warrant: The Disturbing, Unchecked Rise of the Administrative Subpoena', *Wired*, available at: www.wired.com/2012/08/administrative-subpoenas.

2 *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp*, 15 F Supp 3d 466, 468 (SD NY 2014) (hereinafter 'Magistrate Judge's Opinion'). The Magistrate Judge's Opinion, cited throughout, is also freely available at: www.eff.org/files/2014/06/12/magistrate_opinon_re_microsoft_email_warrant.pdf.

3 In this context, latency refers to the risk of slower responsiveness in the use of email (or other internet functions), which may be caused by increased distance between user and server. See http://whatis.techtarget.com/definition/latency.

4 *Ibid.*

5 *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp*, 2014 WL 4629624 (SD NY Aug 29, 2014) (slip copy) (hereinafter 'District Court Opinion').

6 In the federal system, a recipient can challenge a subpoena on the ground that 'compliance would be unreasonable or oppressive': F R Crim P 17(c)(2).

7 As noted, the SCA does not specifically mention 'emails' as such, but rather talks about different varieties of 'stored data.' The application of the SCA to emails, and development of the distinctions noted here relating to age and status as 'opened' or 'unopened' resulted from judicial interpretation. See Magistrate Judge's Opinion at p 6, fn 2; see generally O S Kerr, 'A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It', 72 Geo Wash L Rev 1208 (2004).

8 *United States v Warshak*, 631 F 3d 266, 288 (6th Cir 2010) held that to the extent that the SCA purports to allow the government warrantless access to email content, it is unconstitutional. The *Warshak* ruling has not been tested in the Supreme Court, which suggests that agencies have largely conformed to the decision and sought out SCA 'warrants' rather than subpoenas or court orders.

9 Magistrate Judge's Opinion, 15 F Supp 3d at 470.

10 See, eg *Marc Rich & Co, AG v United States*, 707 F 2d 663, 667 (2d Cir 1983).

11 *Ibid* at 475.

12 *Morrison v National Australia Bank Ltd*, 561 US 247, 255, 130 S Ct 2869, 2878, 177 L Ed 2d 535 (2010).

13 *Kiobel v Royal Dutch Petroleum Co*, —— US ——, ——, 133 S Ct 1659, 1664, 185 L Ed 2d 671 (2013).

14 Magistrate Judge's Opinion, 15 F Supp 3d at 475.

15 This article addresses 'international law' only in the context of the extraterritorial reach of a country's powers. International legal principles may also apply to the rights of individuals. That topic is not addressed in the present article.

16 Restatement (Third) of the Foreign Relations Law of the United States, para 401 et seq. (1987) (hereinafter 'Restatement Third').

17 *SS Lotus (Turk v Fr)*, 1927 PCIJ (ser A) No 10 (Sept 7).
18 Restatement Third, paras 402, 421.
19 *US v Aluminum Co of America*, 148 F 2d 416, 443 (CA 2 1945) (considered to be the first example in US law of the modern effects test).
For a discussion of the effects test under US law *see* Kathleen Hixson, 'Extra Territorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States', 12 Fordham Int'l LJ 127 (1988).
20 *See* Kenneth S Gallant, 'Jurisdiction to Adjudicate and Jurisdiction to Prescribe in International Criminal Courts', 48 Vill L Rev 763, n 214 (2003) for a list of cases in multiple nations around the world where versions of the 'effects test' have been applied.
For a discussion of the effects test under the law of the EU, *see* Laurent Cohen-Tanugi, 'The Extraterritorial Application of American Law: Myths and Realities,' *En temps réel, (*2014), http://laurentcohentanugiavocats.com/press.
21 '[I]n *United States v Odeh*, 552 F 3d 157 (2d Cir 2008), the Second Circuit noted that "seven justices of the Supreme Court [in *United States v Verdugo–Urquidez*, 494 US 259, 110 S Ct 1056, 108 L Ed 2d 222 (1990)] endorsed the view that US courts are not empowered to issue warrants for foreign searches"': Magistrate Judge's Opinion, 15 F Supp 3d at 476 (further holding that such limitations only apply to conventional warrants, not SCA hybrid warrants which do not interfere with foreign territory in the same way).
22 D Anderson, 'A Question of Trust, Report of the Investigatory Powers Review' (June 2015) at p 51, available at: www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review.
23 Paper and other traditional forms of information storage can, of course, be copied. The difference between paper and data copying are primarily two: a copy of data is remarkably cheap to make, store and retrieve; and while a 'copy' of a physical document is almost always different from the 'original', generally speaking there is no such distinction between the 'original' and the 'copy' of digitised information – they are literally identical.
24 D Anderson, op cit, at p 51.
25 Magistrate Judge's Opinion at 475, citing Steven R Swanson, 'Google Sets Sail: Ocean–Based Server Farms and International Law', 43 U Conn L Rev 709, 716–18 (2011).
26 Glenn Fleishman, 'How to keep your email private with PGP encryption on your Mac', *Macworld* at www.macworld.com/article/2890537/how-to-keep-your-email-private-with-pgp-encryption-on-your-mac.html (guide for new users of public-key cryptography tools).
27 For example, France's so-called 'Blocking Statute' makes it a crime to transfer certain kinds of information outside of France for use in an 'administrative or judicial proceeding' other than pursuant to international agreements or conventions. See generally P Grosdidier, 'The French Blocking Statute, the Hague Evidence Convention, and the Case Law: Lessons for French parties responding to American discovery', 50 Tex Int'l L J F 11 (2014).
28 A non-citizen may have certain rights under diplomatic conventions applicable to the country where he is arrested, but that would not affect such a non-citizen's rights during an investigative phase.
29 Microsoft's standing may be questioned. On 21 July 2015 the Appellate Division, First Department, of the Supreme Court of the State of New York ruled on an application by Facebook seeking an order that it should not have to respond to 381 'search warrants' served on it by the District Attorney seeking customer information, arguing a variety of privacy-related and overbreadth issues. The District Attorney challenged Facebook's 'standing' to contest the application for the warrants. Without using the word 'standing' the Appellate Division dismissed Facebook's appeal, noting that the real privacy interests were those of Facebook's customers, and that those interests were sufficiently addressed by the ability of the customers to seek suppression at trial of improperly issued warrants. The case did not involve any international or extraterritorial issues. Microsoft joined a brief filed as *amicus curiae* supporting Facebook. *381 Search Warrants Directed to Facebook, Inc v New York County Dist Attorney's Off*, No 30207/13 30178/14, 2015 NY Slip Op 06201 (NY 1st Dep't July 21, 2015),available at: www.courts.state.ny.us/reporter/3dseries/2015/2015_06201.htm.
30 See, eg P Grosdidier, 'When Internet Libel Lands You in an Out-of-State Court', Law360, 24 April 2015.

CRIMES AGAINST WOMEN SUBCOMMITTEE FEATURES

Persecution on the ground of sexual orientation in international criminal law

INTERNATIONAL

Ruby Axelson
Global Rights Compliance, London
rubymaeaxelson@gmail.com

Having been initially identified as a crime against humanity during the Armenian massacres of 1915, and first prosecuted during the Nuremberg Trials, the criminalisation of 'massacres and other violent conduct against targeted groups'[1] amounting to persecution provides an important opportunity for the protection of marginalised peoples. Focusing on those persons who are, across the globe, persistently subjected to violations of their human rights due to their sexual orientation, this article attempts to situate protection for diverse sexualities under persecution as a crime against humanity in the Rome Statute[2] and to situate the groups identified under Article 7(1)(h) as an *ejusdem generis* list, in order to further facilitate the incorporation of sexual minorities.

The Rome Statute defines persecution as 'the intentional and severe deprivation of fundamental rights contrary to international law by reason of the identity of the group or collectivity', committed in connection with other enumerated acts under the jurisdiction of the International Criminal Court (ICC). Additionally, the persecution must satisfy the chapeau of crimes against humanity, namely that it be 'committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack'.[3] Nevertheless, describing persecution as those acts committed against 'any identifiable group or collectivity on political, racial, national, ethnic, religious, gender… or other grounds universally recognised as impermissible under international law',[4] the Rome Statute represents a clear barrier to protection for sexual minorities.

Despite the possibility that the qualification of gender, which situates gender within the societal roles of men and women, may provide protection for sexual minorities on account of the 'ascribed roles flowing from the assumption of a heterosexual orientation',[5] in reality, the definition fails to adequately distinguish the difference between gender and biological sex. Moreover, while sexual orientation remains markedly absent from international human rights treaties, prospective incorporation of sexual minorities under 'other grounds universally recognised as impermissible under international law' remains significantly curtailed considering that the phrase constitutes a 'higher threshold than requiring that certain distinctions are impermissible under international law in general'.[6] Thus, while these groups represent important avenues to further advocate for protection of sexual minorities, their significant pitfalls necessitate the expansion of the crime of persecution.

The inability to definitively ensure identification of sexual orientation under Article 7(1)(h) necessitates a theoretical grounding of the struggle to achieve equal recognition for sexual diversity, leading to the assertion of a more holistic analysis of how the Rome Statute could better come to protect marginalised groups from persecution. Through the conceptualisation that 'all human beings are born free and equal in dignity and rights',[7] the protection of sexual diversity may be advanced in international criminal law. Understanding that the aims of the ICC to 'protect fundamental human rights by prosecuting and punishing international crimes'[8] are intrinsically linked to the guiding notions of universality and non-discrimination, the failure to proscribe persecution against sexual minorities may be recognised as the dehumanisation of the sexual subject.[9] As such, it has been suggested that the Yogyakarta Principles,

based on conceptions of anti-discrimination and equality, have strong support in existing international law, regional treaties, United Nations conventions and customary law due to the emerging consensus that international human rights law prohibits all arbitrary distinctions.[10] Understanding that sexuality is a basic component of 'human dignity, identity and personhood'[11] incorporates protection for sexual minorities through existing rights, their humanity being dependent on respect for diverse sexuality.

A failure to recognise sexual orientation as a ground for protection would severely undermine the principles of universality and non-discrimination and accordingly act to the detriment of the international community.[12] Indeed, since the crime of persecution is explicitly connected to the 'severe deprivation of fundamental rights', it would consequently be 'difficult for a court to hold that such an egregious crime is permissible under international law',[13] especially in light of the 'object and purpose'[14] of the Rome Statute. A failure to overcome the heteronormativity of international criminal law would ensure that Article 7(1)(h) embodies, like the UN Convention on Genocide[15], a classic 'checkerboard system' that 'provides disparate protection to victims of massive human rights violations on arbitrary grounds',[16] rather than promoting the equal dignity and worth of all humans regardless of sexuality.

Following from these theoretical assumptions, the natural progression is to question why any 'identifiable group or collectivity' should be denied protection under persecution as a crime against humanity. Under the perpetual threat that 'politics will turn cancerous and the indispensable institutions of organised political life will destroy us', all humans share a collective interest in expanding the protection against, and repressing, such crimes.[17] A comprehension that international criminal law may issue persecutors a 'free pass merely because the group they persecute consists of gays or intellectuals, rather than Jews or Tutsis'[18] is theoretically indefensible. Yet, an attempt to fully enumerate possible grounds of persecution is fruitless given that it is impossible to predict with any certainty all of the grounds on which massive human rights violations will be committed in the future.[19]

In much the same way as the 'statutory lists of crimes of the murder type have followed humankind's learning curve in devising new forms of organised atrocities', so too should definitions of persecution continue to follow the learning curve of group discrimination.[20] Since 'progress' in the 'art of hatred' continues to necessitate expansion,[21] it is imperative that the Rome Statute be viewed as a living instrument able to adapt to contemporary needs in the advancement of fundamental human rights, through the recognition that 'there is always further injustice in need of redress'.[22] A more expansive interpretation of 'universally recognised' to include sexual minorities, but also any group suffering an attack that includes the *actus reus* of persecution, is therefore promoted since 'all such attacks are invidious'[23] and such discrimination would surely be prohibited under international law.

While statutory recognition that the grounds of persecution are merely illustrative represents the ultimate goal, an expansive and incremental approach[24] may be achieved through judicial creativity, filling in the 'shortcomings of the Rome Statute's diplomatic compromises'.[25] Referencing persons who were 'killed because of their rank and position in society and their membership of a particular ethnic group or nationality',[26] neither of which were explicitly listed as grounds of persecution,[27] the International Criminal Tribunal for the Former Yugoslavia (ICTY) in *Sikirica* has demonstrated that while 'the requirement of discriminatory intent on one of the listed grounds is not disputed, it is not clear that it has always been followed in practice'.[28] The International Commission of Inquiry on Darfur also acknowledged the importance of expansive interpretation, explaining that from a legal perspective what matters is that expansion 'is in line with the object and scope of the rules of genocide'[29] – a formulation also applicable to persecution given that 'interpretation and expansion has become part and parcel of customary international law'.[30]

Upon these theoretical assumptions, an argument for the grounds of persecution to be viewed as 'illustrative' and able to incorporate the invidious acts committed against any 'identifiable group or collectivity' through judicial interpretation or statutory amendment, may be initiated. It is therefore contended that the ICC should utilise the doctrine of *ejusdem generis*, the idea that specific words should be construed 'consistent with' general words,[31] in order to interpret grounds protected under persecution. Having been previously recognised by the ICTY as a 'common canon of interpretation',[32] Schabas (2000) has articulated that 'general rules of

interpretation would suggest an *ejusdem generis* approach'[33] in the expansion of protected categories under the crime of genocide. As a 'firmly principled framework'[34], *ejusdem generis* negates fears that an 'illustrative' list of protected grounds would be contrary to the essential principle of *nullum crimen sine lege*[35] by offering the ICC the opportunity to give 'meaning to groups of words where one of the words is ambiguous or inherently unclear',[36] thereby ensuring that additional groups would be considered 'on the basis of the same kinds of non-discrimination concerns'[37] that have been shown to underpin international criminal law.

Derogations from the strict application of the principle of *nullum crimen sine lege,* through engagement 'in normative judicial creativity within the boundaries of *ejusdem generis',*[38] enables the ICC to 'balance considerations of fairness towards the accused with other objectives' such as condemnation of brutal acts and the ensurance of individual criminal responsibility.[39] Contending that the grounds of genocide feature a 'common characteristic',[40] the *Akayesu* Trial Chamber has already actively utilised the doctrine, suggesting that the list of enumerated grounds for genocide 'is an *ejusdem generis* list'.[41] This 'traditional method of statutory interpretation'[42] has also found favour in international refugee law, being first utilised in the *Matter of Acosta* to consider that a 'particular social group' was 'a group of persons all of whom share a common, immutable characteristic'.[43] Further elaborating that the characteristic must be something 'the members of the group either cannot change or should not be required to change because it is fundamental to their individual identities or consciences'.[44] By employing the standard of *ejusdem generis* in persecution cases, the ICC may ensure that the interpretation is 'capable of principled evolution but not so vague as to admit persons without a serious basis for claims to international protection',[45] enabling a more holistic approach to the protection of marginalised groups.

It is oft contended that groups worthy of protection in an *ejusdem generis* list of persecuted groups exist as such due to their characteristics of immutability. Indeed, describing the protected grounds under the UN Convention on Genocide as 'stable and permanent groups',[46] the *Akayesu* judgment defined members as unchangeable and defined by birth.[47] Such reasoning was utilised in Beijing in 1995 at the 4th Conference on Women, where the Vatican and Islamic states argued that sexual orientation was a 'non-subject' that would open the floodgates to many 'unacceptable behaviours'.[48] For those arguing that sexual minorities deserve equal protection to those discriminated against because of race or gender,[49] this barrier has regularly led to an ill-placed attempt to situate sexual orientation as an immutable characteristic.[50] However, this reasoning, 'according to which our contemporary categories of sexual orientation can be applied to people in any culture and at any point in history', is implicated in an essentialising rhetoric[51] antithetical to modern understandings of sexuality. A more nuanced understanding of sexual orientation comprehends that 'regardless of whether non-heterosexual or atypical identity is innate or acquired, sexual identity is one of a human being's most personal and essential characteristics',[52] enabling sexual orientation to be properly situated within the protected groups of persecution under an *ejusdem generis* approach.

Neither does an examination of the pre-existing grounds of persecution render immutability necessary. The *Akayesu* formulations neglect the 'freely alienable' characteristics of religion and nationality recognised by the Universal Declaration of Human Rights, rendering the 'Tribunal's perceived analytical distinction between stable and unstable, alienable and inalienable groups… simply intellectually unsatisfactory'.[53] Defined as those who 'share the same religion, domination or mode of worship',[54] religious groups are exemplary of an understanding that persecution can cover behavioural aspects, enabling members to leave, change or join different religions. Protection against discrimination on the basis of a person's political ideology determined by 'behavioural as well as expressed opinion'[55] demonstrates clearly an understanding in international criminal law that, regardless of whether group membership is 'voluntary or innate, individuals should not be forced to surrender their political affiliations or renounce their political beliefs in order to avoid persecution'.[56] These pre-existing understandings of protected groups provide an established formulation available to the ICC to provide for the protection of sexual orientation under an *ejusdem generis* approach. Underlying the protection of political and religious groups lay understandings of

freedom of expression, freedom of association and freedom of conscience;[57] rights that also 'provide a robust defence' for sexual minority protection.[58]

Even the grounds more traditionally understood as immutable provide evidence of behavioural and social aspects.[59] For example, race defined as 'the hereditary physical traits often associated with geographical region'[60] also exemplifies such an understanding. Being an idea traceable to the Spanish Conquest and gaining widespread currency only in the 19th Century, the concept of race attributes to people 'arbitrary classifications that have no basis in biology or any other science', failing to correspond to a 'verifiable reality'.[61] Accordingly, Richards (1994) suggests that race is not a suspect classification on immutable grounds but because 'racial prejudice is an invidious political evil… directed against central aspects of a person's cultural and moral identity',[62] much like prejudice against sexual orientation. Ethnic groups, defined as groups whose 'members share a common language or culture',[63] have also been understood as social constructions lacking 'precisely defined boundaries'.[64] Such mutability is also evident in sexual diversity being understood as a 'continuum that ranges from exclusive heterosexual to exclusive homosexual'.[65]

The fluidity of ethnicity, 'ethnic bonds being more cultural' than those associated with race,[66] was recognised by the International Criminal Tribunal for Rwanda enabling a prosecution on the grounds that 'the racist extremists who perpetrated the genocide saw them as being ethnically distinct', negating concerns over whether the 'Tutsi were in fact ethically distinct from the Hutu, in an objective sense'.[67] A discussion of the already extant protections under Article 7(1)(h) eludes to an *ejusdem generis* understanding of groups exhibiting innate, social and behavioural aspects, limited by the understanding that they correspond to a deep need that is often inescapable for the individual concerned,[68] rendering them 'so fundamental to individual identity or conscience that they ought not be required to be changed'.[69]

A final qualification on the proposed *ejusdem generis* approach requires a return to anti-discrimination notions to ensure that the 'discrimination is invidious enough to be criminalised'[70] and worthy of international protection. Recognising the importance of discriminatory principles in persecution and the formulation of protected groups appreciates that it is the 'history and current existence of discrimination against' sexual minorities that 'qualifies them as a distinct target group eligible for protection under international law'.[71] Such reasoning has been recognised in the European Court of Human Rights (ECtHR), rendering discrimination on account of sexual orientation unjustifiable due to a 'predisposed bias on the part of the heterosexual majority… any more than similar negative attitudes towards those of a different race, origin or colour'.[72]

Noting that sexual minorities 'constitute a distinct though invisible section of the community that has been treated not only with disrespect or condemnation but with disapproval and revulsion',[73] the South African Constitution appreciates the similarities between persecution on account of sexuality, race and ethnicity.[74] Such an understanding recognises that, like other protected classifications, sexual minorities are similarly 'human beings who have been identified by dominant social groups as somehow less than fully human, and thus not entitled to the same rights'[75] although, unlike these protected groups, sexual minorities have failed to gain international recognition of their plight.[76]

Comprehending the a priori enumerated grounds as 'successful struggles',[77] – those groups 'that previously, but no longer, have been systematically… treated as less than full-rights holding members of the political community',[78] – requires continued expansion along *ejusdem generis* grounds essential to the continuing universalisation of international criminal law. Seen as a 'tradition that has transformed a panoply of basic human needs into rights respected',[79] international law necessitates continued recognition of groups facing the *actus reus* of persecution. A struggle existing against a 'dominant oppressive mainstream' has ultimately proved successful for the existent protected grounds 'forcing them to renounce their permissions to hate'; this struggle continues for sexual minorities,[80] but must prove successful for the legitimacy of international law. Viewing the international legal project as 'a process of slowly, with immense difficulty, expanding the recognised subjects of human rights, group by despised group',[81] the *ejusdem generis* approach, focusing on fundamental characteristics that have faced historic discrimination, would equip protection against persecution with the ability to better protect marginalised peoples.

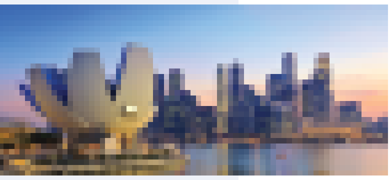
Notes

1 Pocur F (2008) 'Persecution as Crime under International Criminal Law', *Journal of National Security and Policy* 355 (2), p356.
2 UN General Assembly (1998), Rome Statute of the International Criminal Court, A/CONF.183/9, Article 7(1)(h).
3 *Ibid*, Article 7(1).
4 *Ibid*, Article 7(1)(h).
5 Bedont B (1999) 'Gender-Specific Provisions in the Statute of the International Criminal Court' in Lattanzi F and Schabas WA (eds) *Essays on the Rome Statute of the International Criminal Court vol 1* (Editrice il Sirente, Fagnano Alto), pp183-210, p188.
6 Boot M (2002) *Genocide, Crimes Against Humanity, War Crimes: Nullum Crimen Sine Lege and the Subject Matter Jurisdiction of the International Criminal Court* (Intersentia, Antwerpen), p521.
7 UN General Assembly (1948), Universal Declaration of Human Rights, Resolution 217 A (III), Article 1.
8 Ambros K (2013) 'Punishment without a Sovereign? The *Ius Puniendi* Issue of International Criminal Law: A First Contribution Towards a Consistent Theory of International Criminal Law', *Oxford Journal of Legal Studies* 293 (33), p294.
9 UN General Assembly (2011) *Questions of Torture and other Cruel, Inhuman or Degrading Treatment or Punishment: Note by the Secretary General*, A/56/156, para 19.
10 Brown D (2009) 'Making Room for Sexual Orientation and Gender Identity in International Human Rights Law: An Introduction to the Yogyakarta Principles', *Michigan Journal of International Law* 821 (31), p849.
11 Kukuru E (2005) 'Sexual Orientation and Non-Discrimination', *Peace Review: A Journal of Social Justice* 181 (17), p185.
12 *Ibid*, p186.
13 Spees P (2003) 'Women's Advocacy in the Creation of the International Criminal Court: Changing the Landscapes of Justice and Power', *Signs* 1,233 (28), p1,245.
14 United Nations (1969) Vienna Convention on the Law of Treaties, United Nations Treaty Series Vol 1,155, p331, Article 31(1).
15 The Convention on the Prevention and Punishment of the Crime of Genocide.
16 Van Schaack B (1997) 'The Crime of Political Genocide: Repairing the Genocide Convention's Blind Spot', *The Yale Journal of International Law* 2,259 (106), p2,268.
17 Luban D (2004) 'A Theory of Crimes Against Humanity', *Yale Journal of International Law* 85 (29), pp90-91.
18 *Ibid*, p106.
19 deGuzman MA (2000) 'The Road from Rome: The Developing Law of Crimes Against Humanity', *Human Rights Quarterly* 335 (22), p368.
20 See n17, p100.
21 *Ibid*, p100.
22 Dembour M (2010) 'What are Human Rights? Four Schools of Thought', *Human Rights Quarterly* 1 (32), p6.
23 See n17, p106.
24 Hathaway J and Foster M (2003) 'Membership of a Particular Social Group' *International Journal of Refugee Law* 477 (15), p477.
25 Wessel J (2005) 'Judicial Policy-Making at the International Criminal Court: An Institutional Guide to Analyzing International Adjudication', *Columbia Journal of Transnational Law* 377 (44), p381.
26 ICTY (13 November 2001), *Prosecutor v Sikirica* (Sentencing Judgment), (Trial Chamber) IT-95-8-S, para 122.
27 UN Security Council (1994) Statute of the International Criminal Tribunal for the former Yugoslavia, UN Doc SC/Res/827/94, Article 5(h).
28 Roberts K (2002) 'The Law of Persecution before the International Criminal Tribunal for the Former Yugoslavia', *Leiden Journal of International Law* 623 (15), p635.
29 International Commission of Inquiry on Darfur (2005) *Report of the International Commission of Inquiry on Darfur to the United Nations Secretary-General*, Pursuant to Security Council Resolution 1,564 of 18 September 2004, Geneva, para 501.
30 *Ibid*, para 501.
31 Anker D and Ardalan S (2012) 'Escalating Persecution of Gays and Refugee Protection: Comment on "Queer Cases Make Bad Law"', *New York University Journal of International Law and Politics* 529 (44), p543.
32 ICTY (16 November 1998) *Prosecutor v Delalić* (Judgment), (Trial Chamber) IT-96-21-T, para 166.
33 Schabas W (2000) *Genocide in International Law: The Crime of Crimes* (Cambridge University Press, Cambridge), p130.
34 Hathaway J and Foster M (2003) 'Membership of a Particular Social Group', *International Journal of Refugee Law* 477 (15), p481.
35 Jyrkkio T (2011) '"Other Inhumane Acts" as Crimes against Humanity', *Helsinki Law Review*, found at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1871883 [last accessed 21 August 2014].
36 Marouf FE (2009) 'The Emerging Importance of "Social Visibility" in Defining a Particular Social Group and its Potential Impact on Asylum Claims Related to Sexual Orientation and Gender', *Yale Law & Policy Review* 48 (27), p52.
37 See n34, p481.
38 Van Schaack B (2009) 'The Principle of Legality in International Criminal Law: Legality and International Criminal Law', *American Society of International Law Proceedings* 101 (103), p102.
39 *Ibid*, p102.
40 International Criminal Tribunal for Rwanda (2 September 1998), *Prosecutor v Jean-Paul Akayesu* (Judgment), (Chamber I) ICTR-96-4-T, para 511.
41 See n6, p429.
42 See n36.
43 United States Board of Immigration Appeals, *Matter of Acosta* [1985], Interim Decision 2986, A-24159781, p233.
44 *Ibid*, p233.
45 Hathaway JC and Foster (2014) *The Law of Refugee Status (2nd Edition)* (Cambridge University Press, Cambridge), p427.
46 See n40, para 516.
47 *Ibid*, para 511.
48 Saiz I (2004) 'Bracketing Sexuality: Human Rights and Sexual Orientation – A Decade of Development and Denial at the UN', *Health and Human Rights* 48, p58.
49 Heinze E (1995) *Sexual Orientation: A Human Right. An Essay on International Human Rights Law* (Martinus Nijoff Publishers, London), p21.
50 Stein E (2002) 'Law, Sexual Orientation, and Gender' in Coleman J and Shapiro S (eds) *The Oxford Handbook of Jurisprudence and Philosophy of Law* (Oxford University Press, Oxford), pp990-1,039, p991.
51 *Ibid*, p998.
52 Reeves AR (2009) 'Sexual Identity as a Fundamental Human Right', *Buffalo Human Rights Law Review* 215 (15), p255.
53 Nersessian DL (2003) 'The Razor's Edge: Defining and Protecting Human Groups Under the Genocide Convention', *Cornell International Law Journal* 293 (36), p306.
54 Byron C (2004) 'The Crime of Genocide' in McGoldrick D, Rowe P and Donnelly E (eds) *The Permanent International Criminal Court: Legal and Policy Issues (Studies in International Law)* (Hart Publishing, Oxford), pp143-178, p159.
55 UN Division for the Advancement of Women, Department of Economic and Social Affairs (1997) *Gender-Based Persecution: Report of the Expert Group Meeting*, EGM/GBP/1997, para 44.

56 See n16, p2,288.
57 UN General Assembly (1966) International Covenant on Civil and Political Rights, Treaty Series vol 999, p171, Article 19 (2), Article 22 and Article 18.
58 See n50, p1,039.
59 Richards DAJ (1994) 'Sexual Preference as a Suspect (Religious) Classification: An Alternative Perspective on the Unconstitutionality of Anti-Lesbian/Gay Initiatives', *Ohio State Law Journal* 491 (55), p505.
60 See n40, para 514.
61 Keane D (2007) *Caste-Based Discrimination in International Human Rights Law* (Ashgate Publishing, Hampshire), p11.
62 See n59, p502-504.
63 See n40, para 513.
64 See n54, p158.
65 Mutua M (2011) 'Sexual Orientation and Human Rights: Putting Homophobia on Trial' in Temale S (ed) *African Sexualities* (Pambazuka Press, Cape Town), pp452-462, p457.
66 Thiam D, Special Rapporteur (1986) *Fourth Report on the Draft Code of Offenses Against the Peace and Security of Mankind*, A/CN.4/398 and Corr 1-3, para 58.
67 Schabas WA (2005) 'Genocide, Crimes Against Humanity, and Darfur: The Commission of Inquiry's Findings on Genocide', *Cardozo Law Review* 1,703 (27), p1,713.
68 Waaldijk K (2013) 'The Right to Relate: A Lecture on the Importance of "Orientation" in Comparative Sexual Orientation Law', *Duke Journal of Comparative and International Law* 161 (24), p165.
69 See n43, p533.
70 See n17, p106.
71 Brydum S (2013) 'Scott Lively Will be Tried for Fueling Antigay Persecution in Uganda', found at www.advocate.com/news/world-news/2013/08/15/scott-lively-will-be-tried-fueling-antigay-persecution-uganda [Last accessed 21 August 2014].
72 Council of Europe, ECtHR (1990), *Smith and Grady v UK*, Application No 33985/96 and 33986/96, para 97.
73 South African Constitutional Court, *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others* [1998], CCT 11/98, para 128.
74 International Commission of Jurists (2009) *Sexual Orientation, Gender Identity and International Human Rights Law: Practitioners Guide No.4*, International Commission of Jurists, Geneva, p5, citing Archbishop Desmond Tutu.
75 Donnelly J (1999) 'Non-Discrimination and Sexual Orientation: Making a Place for Sexual Minorities in the Global Human Rights Regime' in Baehr P, Flintermann C and Senders M (eds) *Innovation and Inspiration: Fifty Years of the Universal Declaration of Human Rights* (Royal Netherlands Academy of Arts and Sciences, Amsterdam), pp93-110, p98.
76 DeLaet DL (1997) 'Don't Ask, Don't Tell: Where is the Protection Against Sexual Orientation Discrimination in International Human Rights Law', *Law and Sexuality: Review of Lesbian, Gay, Bisexual and Transgender Legal Issues* 31 (7), p32.
77 See n75, p95.
78 *Ibid*, p95.
79 Helfer LR and Miller AM (1996) 'Sexual Orientation and Human Rights: Toward a United States and Transnational Jurisprudence', *Harvard Human Rights Journal* (9), p85.
80 See n75, p107.
81 *Ibid*, p95.

International Bar Association

Conferences 2015–2016




[illegible] NOVEMBER 2015 | [illegible]

Asia-Pacific Arbitration Group Training Day—[illegible] in International Arbitration

10 NOVEMBER 2015 | MOSCOW, RUSSIA

[illegible] Annual Mergers and Acquisitions in Russia and CIS Conference

10 NOVEMBER 2015 | LONDON, ENGLAND

Private Equity Transactions Symposium

13 NOVEMBER 2015 | SÃO PAULO, BRAZIL

Celebrating Magna Carta and the Rule of Law

[illegible]

IBA-ELSA Law Students' Conference 2015

[illegible]

[illegible]

[illegible]

[illegible] Global [illegible] Conference

[illegible]

[illegible]

[illegible]

[illegible]

9–11 DECEMBER 2015 | MEXICO CITY, MEXICO

The New Era of Taxation: The keys to providing legal advice on taxation in a rapidly changing world

[illegible] | [illegible], JAPAN

[illegible] Annual Law Firm Management Conference

[illegible]

The Rise of Ethics and Transparency in [illegible]: Fighting Corruption and Abuses through [illegible]

[illegible]

Magna Carta [illegible]

[illegible] 2016 | MEXICO CITY, MEXICO

[illegible] Energy Reform: The [illegible]

[illegible] 2016
[illegible]

Legal Challenges of Modern Warfare

[illegible] FEBRUARY 2016 | TOKYO, JAPAN

[illegible] International Cartel Workshop

[illegible] FEBRUARY 2016 | LONDON, ENGLAND

[illegible] Annual IBA Taxation Conference

17–18 MARCH 2016 | PARIS, FRANCE

[illegible] IBA European Corporate and Private M&A Conference

[illegible] MARCH 2016
[illegible]

Innovation in Legal Practice

[illegible]

[illegible] Annual International [illegible] Law Conference

[illegible] | [illegible]

[illegible] Annual International [illegible]

[illegible] 2016 | [illegible]

[illegible] Annual International Conference on Private Investment Funds

[illegible] 2016 | [illegible], BRAZIL

[illegible] Latin American Regional Forum Conference

[illegible] MARCH 2016 | SINGAPORE

2nd Asia-based International Financial Law Conference

7–8 APRIL 2016 | BERLIN, GERMANY

7th World Women Lawyers' Conference

14–15 APRIL 2016 | COPENHAGEN, DENMARK

4th Annual Real Estate Investment Conference

[illegible] APRIL 2016 | MEXICO CITY, MEXICO

IBA Annual Employment and [illegible] Law Conference

[illegible] 2016 | NEW YORK, USA

[illegible] Conference of the Section on Energy, Environment, Natural Resources and Infrastructure Law

[illegible] 2016 | SAN FRANCISCO, USA

IBA Annual Litigation Forum 2016

Full and further information on upcoming IBA events for 2015/2016 can be found at: bit.ly/IBAConferences