Pandora's Box

2016 *Law and Technology*

A publication of the Justice and the Law Society
THE UNIVERSITY OF QUEENSLAND

Pandora's Box

2016 *Law and Technology*

Editors

Madeleine Gifford & Michael Potts

ISSN: 1835-8624
Published by:
The Justice and the Law Society
T.C. Beirne School of Law
The University of Queensland
St Lucia QLD 4072
www.jatl.org

Printed by:
Worldwide Printing
Fortitude Valley

SPONSORS

This edition of *Pandora's Box* would not have been possible without the generous support of the *Queensland Law Society* and the fundraising efforts of the 2016 JATL Executive.

TABLE OF CONTENTS

'As the custodians of the law, we not only have a responsibility to be at the forefront in the innovation and application of that kind of new technology but we also have reason to be excited about the benefits which it is likely to yield.'

-- Geoffrey Nettle, *Technology and the Law*, speech delivered on 27 February 2016 at the Bar Association of Queensland Annual Conference, Queen Elizabeth II Courts of Law, Brisbane.

FOREWORD

Sarah Derrington*

The importance of Law and Technology has grown rapidly over the recent decades, not merely as a matter of substantive law but also in the context of the practice of law. Modern law firms are grappling with the integration of highly sophisticated technologies such as artificial intelligence and what that might mean for future practitioners. The modern lawyer must contend with e-files, e-discovery and e-courts, with e-project management tools, with automation and cybersecurity issues, all in the context of rapidly changing client expectations about the speed, form and efficiency of the delivery of legal services.

Understanding the legal issues around technology in all its forms is the subject matter of this edition of *Pandora's Box*, which is both timely and thought provoking. The Editors are to be congratulated for their foresight in choosing such an important theme and for producing a collection of papers that are thought provoking and of immense current interest.

* Professor, Academic Dean and Head of School, TC Beirne School of Law, University of Queensland.

THE FUTURE IS NOW

Bill Potts*

The great myth of our times is that technology is communication.
– Libby Larsen (Composer)

Much has changed in both the world and the law since my admission in 1982. In my day, law firms had phones, but now phones have law firms on them and you can access your email from the palm of your hand. You can file documents and complete conveyances online that once upon a time took weeks to arrange and may be cancelled because there was an extra full stop on the cheque.

Technology can support the legal profession in many ways, but can it completely replace the traditional lawyer and law firm?

The philosopher Jacques Ellul once said: "Modern technology has become a total phenomenon for civilization, the defining force of a new social order in which efficiency is no longer an option but a necessity imposed on all human activity."[1]

This type of efficiency is a great thing for lawyers, and assists us to help clients in faster, better and more affordable ways. It can also connect us with clients who may not have been exposed to your firm had it not been for an internet search or social media account. Although, lawyers are typically a very traditional cohort, we remain aware of changes in the profession and in society as a whole.

Lawyers are often seen as being behind the trend when it comes to technology due to the slow uptake of new platforms and technologies by firms. There have even been warnings that law firms will be overtaken by online consultancy platforms or that senior staff will be replaced by artificial intelligence and junior staff.

In the past few years we have seen an increasing number of online platforms offering legal advice or services at a discount to traditional law firms. Although

---

* President, Queensland Law Society.

[1] Darrell J Fasching, *The Thought of Jacques Ellul: A Systematic Exposition* (Edwin Mellen Press, 1981) 15.

these cookie cutter solutions do not take the place of the role of a trusted adviser, many members of the public view price as a priority when choosing a law firm.

Customers are now able to view legal information at the press of a button on the internet, making the public feel that they are now more informed than they once were. This can encourage customers to seek out the online platforms for advice rather than a face-to-face consult with a lawyer.

Of course, there are positives to the creation of interactive online technologies, with lawyers being able to connect with customers through videos, blogs, podcasts and online chat services. Social media is also being used well by many law firms and individual lawyers, making them seem much more human and real to prospective clients.

But can they replace the traditional law firm? I believe that there will also be a place for the trusted adviser, but as lawyers we will need to be able to work with technology and adapt our firm structure to suit changing needs.

While some of us view these impending changes with reluctance, many of us understand that it is necessary to avoid becoming irrelevant. The Queensland Law Society embraces change and continually looks at better and more efficient ways to connect with members and improve our offerings using a combination of traditional and new mediums.

As we see more law firms embracing technology through more advanced websites with online chat options or interactive bots, social media accounts, embedded videos or podcasts, and the option of webinars, Queensland Law Society is also delving deeper into technology.

What does the future hold? At the Society, we see the future as already being here. We are ensuring that we have the right people in our organisation to drive us forward into that future. Having these specialists will assist us in remaining relevant and connected to our profession. Whether that be through the way we deliver professional development opportunities, connect with our members, and alternative methods disseminating important information.

As a profession, we will face this impending future together. I look forward to seeing where our profession lies in 5, 10 or even 20 years from now.

A NOTE FROM THE EDITORS

The law is sometimes viewed as being 'reactionary', 'slow' or 'backwards looking'. However this view discounts the wealth of innovative and forward-looking academia that is constantly being produced. Numerous strategies have already been proposed that would revolutionise the law as it currently exists. For example, the justice system is often accused of being inaccessible and costly, but by embracing new technologies such as online dispute resolution and virtual courts, wider access to justice may become a reality. The use of artificial intelligence and big data in law firms will increase efficiency, but also disrupt the very nature of legal practice as we know it. It will be imperative that the current generation of law students approach the profession in an innovative and flexible manner.

This year's edition features a diverse range of contributors from across the globe. The common theme throughout many of the articles is the need for global solutions to global problems. Isolated policies for issues such as cybercrime and data privacy are unworkable in the digital age. International co-operation is needed to further global development. Cross-boarder public and private partnerships can create successful patent programs to develop and distribute fortified and therapeutic foods to treat malnutrition, and drugs to combat disease. Innovative copyright regimes could allow people from across the globe access to educational materials and replicate artefacts through 3D printing. These are just some of the solutions presented by our contributors that promote the equal and just adoption of new technologies.

The goal of this edition is to ask difficult questions that often do not have a clear answer. For example, the right to data privacy is continuously being challenged by the adoption of new technologies. It can be difficult to provide protections against constantly developing intrusions, yet comprehensive solutions have been proposed. On the other hand, regulating robotics may be extremely difficult as there is no consensus on how future developments will unfold. It is unknown what rights we should give to robots and what their future role within society will be. Questions on issues such as these are of great importance as they deal with what the future of society may hold. A lack of consensus may also arise in regards to topics such as genomics research, a topic that will also have profound legal ramifications. As the former Justice Michael Kirby notes "the genome, manipulated, has the potential even to change who human beings are. In this respect, it concerns the human rights of

future generations and who humans and future generations will be".[1] Though these topics may seem abstract now, they will have profound ramifications in the future. It is through collections like this one that new ideas and thinking can prepare us to deal with the inevitable change the passage of time will bring.

We'd like to thank everyone who has helped make this year's edition possible. Particular thanks must be directed to our sponsors, the *Queensland Law Society,* for their continued and generous support. Our thanks goes out to Dr Mark Burdon and Professor Brad Sherman for their guidance and help, particularly in regards to this year's Essay Competition. We would also like to thank the entire *JATL* executive for giving us the opportunity to edit this volume and for all their support. Most importantly, we would like to thank our distinguished contributors for their insightful and innovative submissions. We certainly enjoyed editing *Pandora's Box 2016*. We hope that you enjoy reading it.

Madeleine Gifford and Michael Potts
Editors, *Pandora's Box* 2016

ABOUT PANDORA'S BOX

Pandora's Box is the annual academic journal published by the Justice and the Law Society (JATL) of the University of Queensland. It has been published since 1994 and aims to bring academic discussion of legal, social justice and political issues to a wider audience.

Pandora's Box is not so named because of the classical interpretation of the story: of a woman's weakness and disobedience unleashing evils on the world. Rather, we regard Pandora as the heroine of the story – the inquiring mind - as that is what the legal mind should be.

Pandora's Box journal is registered with Ulrich's International Periodical Directory and can be accessed online through *Informit* and EBSCO.

Pandora's Box is launched each year at the Justice and the Law Society's *Annual Professional Breakfast.*

Additional copies of the journal, including previous editions, are available. Please contact pandorasbox@jatl.org for more information or go online at http://www.jatl.org/ to find the digitised versions.

---

[1] Michael Kirby, *Freedom of Information: The Seven Deadly Sins*, speech delivered on 17 December 1997, at the Britsih Section of the International Commission of Jurists Fortieth Anniversary Lecture Series, London.

ABOUT THE CONTRIBUTORS

Sarah Derrington is the Academic Dean and Head of School of the T C Beirne Schoool of Law. With James M Turner QC of the English Bar, she has written one of the leading common law texts on admiralty law and practice and has published widely on matters relating to carriage of goods by sea, marine insurance and admiralty jurisdiction. Professor Derrington has taught a variety of courses in marine and shipping law from undergraduate to postgraduate level and has successfully supervised doctoral candidates in the field. Professor Derrington's work is cited regularly in the Superior Courts, not only within Australia but also in the Courts of the United Kingdom, Hong Kong and Singapore. Her particular expertise in maritime and shipping law has been recognised, domestically, by her appointment to the Admiralty Rules Committee and, internationally, by appointments to International Working Groups of the Comité Maritime International, by instructions to participate in an amicus curiae brief to the Supreme Court of the United States and through her invitation to become a Door Tenant of Quadrant Chambers in London. Professor Derrington continues to practise at the private Bar, exclusively in shipping law.

Angus Fraser is a BA/LLB candidate at the TC Beirne School of Law, The University of Queensland. He was the winner of the Justice and the Law Society's Law and Technology Essay Competition 2015.

Stuart Hargreaves is a Professor and Director of the LLB programme and Assistant Dean for Undergraduate Studies at the Faculty of Law, Chinese University of Hong Kong. He joined the Faculty in July of 2013 following the completion of his doctorate in law at the University of Toronto. He also holds a BCL from Oxford University, a JD from Osgoode Hall Law School, and a BA in politics & sociology from McGill University. He has worked as a policy advisor to the Canadian Internet Policy and Public Interest Clinic and served as counsel to the Ontario Ministry of the Attorney General, in the constitutional law and policy branch. His research and teaching mirrors this background, with a twin emphasis on both information & privacy law and constitutional law and legal theory.

Fabian Horton is a PhD Candidate at Southern Cross University, a lecturer at the College of Law, Melbourne, and a solicitor with extensive experience in legal technologies, online legal applications and social media. He operates his own private virtual firm and is currently undertaking his PhD researching how technology's influences on the law. Fabian is the foundation chairperson of the Technology and the Law Committee of the Law Institute of Victoria.

Keith Kaplan is the Assistant Court Administrator for Phoenix Municipal Court, one of the largest courts in the state of Arizona. Previously, Mr. Kaplan was the Court Administrator for Fountain Hills Municipal Court, a limited jurisdiction court in the Phoenix metropolitan area, where he oversaw and managed all non-judicial decision making and all administrative functions of the court. Mr. Kaplan earned his Bachelor of Science in Justice Studies from Arizona State University and Master of Science in Legal Administration with a Court Administration concentration from University of Denver's Sturm College of Law where he was awarded the Outstanding MSLA Graduate Award. Mr. Kaplan is a Certified Court Manager and Certified Court Executive from the National Center for State Court's Institute Court Management, and is currently a candidate for ICM Fellow from the Institute for Court Management. Mr. Kaplan is also an Adjunct Professor for the University of Denver's Sturm College of Law's Master of Science in Legal Administration program and teaches Managing Court Financial Resources for the Institute for Court Management's Certified Court Manager program.

Xingan Li has been an Associate Professor at Tallinn University, School of Governance, Law and Society, Estonia since 2014. He holds an LLB and LLM from China, an LLD and a PhD in computer science both from Finland. He worked as an assistant professor, lecturer, and associate professor at Inner Mongolia University Law School, China, visiting scholar at Kyushu University's College of Law, Japan, researcher at University of Lapland, researcher, guest lecturer, and postdoctoral researcher at University of Turku, Finland, 2006-2012, and researcher at University of Tampere, Finland. He is also a Distinguished Research Fellow at Beihang University Law School, China. His primary research interests are social order in cyberspace, cyber security and cybercrime, and data mining in research of crime.

Marie-Helen Maras is an Associate Professor at the Department of Security, Fire, and Emergency Management, part of the John Jay College of Criminal Justice. She is the new Fire Science/Fire and Emergency Services advisor. She has a DPhil in Law and an MPhil in Criminology and Criminal Justice from the University of Oxford. In addition, she holds a graduate degree in Industrial and Organizational Psychology from the University of New Haven and undergraduate degrees in Computer and Information Science and Psychology from the University of Maryland University College. She has taught at New York University and SUNY-Farmingdale. In addition to her teaching and academic work, her background includes approximately seven years of service in the U.S. Navy with significant experience in security and law enforcement from her posts as a Navy Law Enforcement Specialist and Command Investigator.

Stephen Mason is a barrister. He was called to the Bar by the Honourable Society of the Middle Temple in November 1988. Stephen is the recognised authority on electronic signatures and digital evidence, and has assisted governments and businesses across the globe.

Bryan Mercurio is a Professor and the Vice Chancellor's Outstanding Fellow of the Faculty of Law at The Chinese University of Hong Kong. He is a leading expert in the field of international economic law (IEL), with a particular interest in WTO law, the intersection between IEL and intellectual property rights, free trade agreements and increasingly international investment law.

Eliza Mik is an Assistant Professor of Law at Singapore Management University. Her research focuses on how the law interacts with contracts, information technology and the internet.

Elizabeth Siew-Kuan Ng is the Deputy Chairwoman and Director (Intellectual Property Research Unit), Centre for Law and Business; Director, Graduate Certificate of Intellectual Property program (GCIP); Associate Professor of Law, Faculty of Law, National University of Singapore; LL.B (Hons) University of London; LL.M (First Class) University of Cambridge; Barrister-at-Law (Middle Temple, London); Advocate & Solicitor (Singapore).

Bill Potts is a solicitor and President of the Queensland Law Society for 2016. He was admitted to practice in 1982 and is the founder of Potts Lawyers, practicing primarily in criminal law.

Megan Richardson is a Professor of Law at the Melbourne Law School, The University of Melbourne. Her fields of research and publication include intellectual property, privacy and personality rights, law reform and legal theory. She was one of a group of scholars convened by the Australian Law Reform Commission to explore the meaning of 'privacy' for its 2006-8 privacy reference, and in addition served on the international advisory panel for the New South Wales Law Reform Commission's invasion of privacy review in 2006-2009. She was also a member of the advisory committee for the Australian Law Reform Commission's reference on Serious Invasions of Privacy in the Digital Era (report published 2014). She is currently Co-Director of the Melbourne Law School's Centre for Media and Communications Law (CMCL) and the Intellectual Property Research Institute of Australia (IPRIA).

Dr Matthew Rimmer is a Professor in Intellectual Property and Innovation Law at the Faculty of Law in the Queensland University of Technology (QUT). He is a leader of the QUT Intellectual Property and Innovation Law research program, and a member of the QUT Digital Media Research Centre (QUT

DMRC), the QUT Australian Centre for Health Law Research (QUT ACHLR), and the QUT International Law and Global Governance Research Program (QUT IL GG). Rimmer has published widely on copyright law and information technology, patent law and biotechnology, access to medicines, plain packaging of tobacco products, intellectual property and climate change, and Indigenous Intellectual Property. He is currently working on research on intellectual property, the creative industries, and 3D printing; intellectual property and public health; and intellectual property and trade, looking at the Trans-Pacific Partnership, the Trans-Atlantic Trade and Investment Partnership, and the Trade in Services Agreement. His work is archived at Bepress Selected Works, Open Science Framework, QUT ePrints, and SSRN Abstracts.

Burkhard Schafer studied law, logic, theory of science and computer linguistics in Germany, Italy and the UK. He has been since 1996 at the School of Law of the University of Edinburgh, since 2010 as Chair of Computational Legal Theory. In Edinburgh, he helped founding two new research centres, the Joseph Bell Centre for Forensic Statistics and Legal Reasoning and the SCRIPT Centre for IT and IP law, which he leads as Director since 2010. His main interest is the interaction between law, science and technology, covering both technology as a subject of regulation and as a tool to improve the justice system. He is member of the Ethics Steering Group of the Alan Turing Institute and member of the ethics board of IMI-EMIF.

Brad Sherman is a Professor of Law at The University of Queensland. His research expertise encompasses many aspects of intellectual property law, with a particular emphasis on its historical, doctrinal and conceptual development. In 2015 Brad was awarded a highly prestigious Australian Research Council Laureate Fellowship. His laureate project *Harnessing Intellectual Property to Build Food Security* looks at the role of intellectual property in relation to food security.

Zheng Sophia Tang is a Professor in Law and Commerce at Newcastle University, a Barrister and an accredited mediator. She is specialised in conflict of laws, electronic consumer protection and commercial dispute resolution, and has published numerous articles and four monographs. She serves as an external expert for the European Commission DG Justice in the Justice programme.

Anne Wallace is a Professor at the School of Business and Law, Edith Cowan University. Anne was the Deputy Executive Director for the Australian Institute of Judicial Administration from 1993 to 2006, where she developed a research interest in the field of judicial administration. Working with the Court

of the Future Network, she has acted as Chief Investigator in two multi-disciplinary research projects that investigate the use of technology in the justice system.

Lu Xu is a PhD candidate at the University of Leeds and her research project is funded by CSC-UoL scholarship. She obtained a LLM from Huazhong University of Science and Technology (Wuhan, China), a LLM from China University of Political Science and Law (CUPL) (Beijing) and has worked as an executive editor of Graduate Law Review in CUPL.

3D Printing Jurassic Park: Copyright Law, Cultural Institutions, and Makerspaces

Matthew Rimmer*

I INTRODUCTION

3D printing is a field of technology, which enabled the manufacturing of physical objects from three-dimensional digital models.[1]

The discipline of copyright law has been challenged and disrupted by the emergence of 3D printing and additive manufacturing. 3D Printing poses questions about the subject matter protected under copyright law. Copyright law provides for exclusive economic and moral rights in respect of cultural works – such as literary works, artistic works, musical works, dramatic works, as well as other subject matter like radio and television broadcasts, sound recordings, and published editions. Copyright law demands a threshold requirement of originality. There have been sometimes issues about the interaction between copyright law and designs law in respect of works of artistic craftsmanship. In addition, 3D printing has raised larger questions about copyright infringement. There has been significant debate over the scope of copyright exceptions – such as the defence of fair dealing, and exceptions for cultural institutions. Moreover, there has been debate over the operation of digital copyright measures in respect of 3D printing. The takedown and notice system has affected services and sites, which enable the sharing of 3D printing designs. Technological protection measures – digital locks – have also raised challenges for 3D printing. The long duration of copyright protection in Australia and the United States has also raised issues in respect of 3D printing.

There has been great public policy interest into how copyright law will address and accommodate the disruptive technologies of 3D Printing. As a public policy expert at Public Knowledge, and as a lawyer working for Shapeways, Michael Weinberg has written a number of public policy papers on intellectual property and 3D Printing.[2] Associate Professor Dinusha Mendis and her

---

* Professor, Faculty of Law, Queensland University of Technology.

[1] Anna Kaziunas France, *Make: 3D Printing. The Essential Guide to 3D Printers* (Maker Media Inc., 2013); Christopher Barnatt, *3D Printing: The Next Industrial Revolution, Explaining the Future* (CreateSpace Independent Publishing Platform, 2013).

[2] Michael Weinberg, *It Will Be Awesome If They Don't Screw It Up: 3D Printing, Intellectual Property, and the Fight over the Next Great Disruptive Technology* (10 November 2010) Public Knowledge

colleagues have undertaken legal and empirical research on intellectual property and 3D printing.[3] In 2015, Professor Mark Lemley from Stanford Law School wrote about intellectual property and 3D printing in the context of work on the economics of abundance.[4] As a practising lawyer, John Hornick has examined the topic of intellectual property and 3D printing.[5] Comparative legal scholar Dr Angela Daly has written on the socio-legal aspects of 3D printing in 2016.[6] The World Intellectual Property Organization in 2015 highlighted 3D printing.[7]

3D printing has provided new opportunities for cultural institutions to redefine their activities and purposes, and engage with a variety of new constituencies. 3D printing has also highlighted deficiencies in copyright law in respect of cultural institutions. Culturally and technologically specific exceptions for libraries, archives, and cultural institutions have proven to be ill-adapted for an age of 3D printing and makerspaces. The Australian Law Reform Commission has highlighted the need to modernise Australia's copyright laws for the digital age.[8] Likewise, the Productivity Commission has considered the question of copyright exceptions in its study of intellectual

---

<https://www.publicknowledge.org/files/docs/3DPrintingPaperPublicKnowledge.pdf>; Michael Weinberg, *What's the Deal with Copyright and 3D Printing*? (29 January 2013) Public Knowledge <https://www.publicknowledge.org/news-blog/blogs/whats-the-deal-with-copyright-and-3d-printing>; Michael Weinberg, *3D Scanning: A World Without Copyright* (May 2016) Shapeways <http://www.shapeways.com/wordpress/wp-content/uploads/2016/05/white-paper-3d-scanning-world-without-copyright.pdf>.

[3] Dinusha Mendis, 'Customising the Future Through New Business Models: The Impact of 3D Printing and 3D Scanning on Mass Customisation and its Implications for Copyright Law' (2015) *Script-ed* 1; Dinusha Mendis, 'Networks of Power in Digital Copyright Law and Policy; Political Salience, Expertise and the Legislative Process' (2015) 37(7) *European Intellectual Property Review* 474; Dinusha Mendis, Davide Secchi, and Phil Reeves, *A Legal and Empirical Study into the Intellectual Property Implications of 3D Printing* (March 2015) Intellectual Property Office <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/421222/A_Legal_and_Empirical_Study_into_the_Intellectual_Property_Implications_of_3D_Printing_-_Exec_Summary_-_Web.pdf>; Davide Secchi and Dinusha Mendis, *A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour* (19 March 2015) UK Intellectual Property Office <https://www.gov.uk/government/publications/a-legal-and-empirical-study-of-3d-printing-online-platforms-and-an-analysis-of-user-behaviour-study-1>.

[4] Mark Lemley, 'IP in a World Without Scarcity' (2015) 90 *New York University Law Review* 460.

[5] John Hornick, *3D Printing Will Rock the World* (CreateSpace, 2015).

[6] Angela Daly, *Socio-Legal Aspects of the 3D Printing Revolution* (Palgrave Pivot, 2016).

[7] World Intellectual Property Organization, *World IP Report: Breakthrough Innovation and Economic Growth* (2015) <http://www.wipo.int/export/sites/www/econ_stat/en/economics/wipr/pdf/wipr_2015_chapter3.pdf>.

[8] Australian Law Reform Commission, *Copyright and the Digital Economy*, Report No 122 (February 2014) <http://www.alrc.gov.au/publications/copyright-report-122>.

property arrangements in 2016.[9] The Turnbull Government has contemplated somewhat more modest copyright reforms, with the draft legislation in the *Copyright Amendment (Disability Access and Other Measures) Bill* 2016 (Cth). Libraries, galleries, museums, and archives would all benefit from flexible copyright exceptions for cultural institutions to take full advantage of the possibilities of digitisation and 3D printing.

II LIBRARIES

Historically, libraries, galleries, museums, and cultural institutions have been embroiled in larger conflicts over copyright law and policy. In 1975, the High Court of Australia considered copyright law and authorisation in the context of disputes of the photocopier.[10] In 2004, the Supreme Court of Canada handed down a landmark ruling in respect of copyright law and libraries.[11] The decision explored originality, authorisation, the defence of fair dealing, and larger questions about access to justice. The United States has long had conflicts in respect of copyright law and cultural institutions.[12] In contemporary times, there has been copyright litigation in respect of large-scale digitisation projects. Libraries – and their commercial partners – have been able to rely upon the defence of fair use.[13]

In his recent book, *BiblioTech*, John Palfrey discusses the need to revise copyright laws for the digital age to better accommodate the role of libraries, galleries, museums, and cultural institutions.[14] He laments: 'The law of copyright, which dates back to the founding of the United States (and beyond, to the Statute of Anne in early-eighteenth-century England), has become just

---

[9] Productivity Commission, *Intellectual Property Arrangements – Draft Report* (April 2016) <http://www.pc.gov.au/inquiries/current/intellectual-property/draft/intellectual-property-draft.pdf>.

[10] *University of New South Wales v Moorhouse* [1975] HCA 26; (1975) 133 CLR 1.

[11] *The Law Society of Upper Canada v CCH Canadian Limited* (2004) SCC 13. For commentary, see Abraham Drassinower, *What's Wrong with Copying?* (Harvard University Press, 2015); Carys Craig, *Copyright, Communication, and Culture: Towards a Relational Theory of Copyright Law* (Edward Elgar Publishing, 2011); Michael Geist (ed), *From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda* (Irwin Law, 2010); Michael Geist (ed), *In The Public Interest: The Future of Canadian Copyright Law* (Irwin law, 2005); Michael Geist (ed.) *The Copyright Pentalogy: How the Supreme Court of Canada shook the Foundations of Canadian Copyright Law* (University of Ottawa Press, 2013).

[12] Peter Hirdle, Emily Hudson and Andrew Kenyon, *Copyright and Cultural Institutions: Guidelines for Digitization for U.S. Libraries, Archives, and Museums* (Cornell University Library, 2009).

[13] *The Authors Guild v HathiTrust* 755 F 3d 87 (2nd Cir, 2014); *The Authors Guild* v *Google Inc.* 804 F 3d 202 (2nd Cir, 2015).

[14] John Palfrey, *BiblioTech: Why Libraries Matter More Than Ever in the Age of Google* (Basic Books, 2015).

such a hindrance when it comes to building strong libraries in a digital era.'[15] Palfrey observed that 'librarians have been at the forefront of efforts to update the law to support their good works into the future.'[16] He hoped that 'the challenges of the digital era for libraries can be addressed in part through smart legal reforms.'[17] Palfrey regretted that 'too few people give voice to the public interest, and the world of knowledge and information is becoming increasingly controlled by corporations.'[18] Accordingly, he concluded: 'Just as we, the public, need to make the case for libraries, we all need the library profession to help make the case for a sensible, public-friendly copyright and privacy regime for the digital era.'[19]

Kenneth Crews has undertaken comprehensive surveys of copyright limitations and exceptions for libraries and archives.[20] He commented that 'exceptions for libraries and archives are fundamental to the structure of copyright law throughout the world, and that the exceptions play an important role in facilitating library services and serving the social objectives of copyright law.'[21] Kenneth Crews has highlighted that there need to be revisions in respect of exceptions for cultural institutions in light of changing needs and new technologies.

The *Copyright Amendment (Disability Access and Other Measures) Bill* 2016 (Cth) also proposes reforms in respect of copyright exceptions for public libraries, parliamentary libraries, and public archives.

Section 113H of the *Copyright Amendment (Disability Access and Other Measures) Bill* 2016 (Cth) provides that an authorised officer of a library or an archives does not infringe copyright by using material for the purpose of preserving the collection comprising the library or archives. This measure is subject to further procedural qualifications.

This reform is designed to address the rather clumsy way that Australian copyright law deals with cultural preservation. The moral rights regime has a clearcut exception for preservation. However, the system of economic rights has not dealt with the issue very clearly thus far.

---

[15] Ibid 182.
[16] Ibid 182.
[17] Ibid 204.
[18] Ibid 205.
[19] Ibid 205.
[20] Kenneth Crews, *Standing Committee on Copyright and Related Rights*, WIPO SCCR/30/3 (10 June 2015) (Study on Copyright Limitations and Exceptions for Libraries and Archives: Updated and Revised) <http://www.wipo.int/edocs/mdocs/copyright/en/sccr_30/sccr_30_3.pdf>.
[21] Ibid 6.

In the United States, there has been enthusiasm about turning public libraries into makerspaces. Richard Reyes-Gavilan, the executive director of the D.C. Public Library system has been interested in revitalising spaces.[22] He has advocated the adoption of a 'hacker' culture, which treats library patrons as creators, rather than passive consumers of information.[23] In his view, 'libraries are not their buildings,' but 'engines of human capital.'[24] Reyes-Gavilan comments that 'Libraries need more tinkerers'.[25] His hope is that such a model will be adopted elsewhere throughout the United States. Ricky Riberio comments that public libraries are turning to 3D printing and technology to transform how they serve their communities. [26]

The British Library has been experimenting with 3D scanning and 3D printing its collection.[27]

3D printing will help transform libraries into sites of creative innovation and experimentation. Mark Hatch has called for a more plentiful supply of makerspaces: 'Fabrication shops will become like libraries, medical clinics, and gymnasiums at universities'.[28]

The State Library of Queensland has been innovative, setting up an experimental library called The Edge, on the banks of the Brisbane River. The Creative Director of The Edge, Daniel Flood, reflected: 'Seemingly every ten years libraries ask themselves: 'what does the library of the future look like?'.[29] He comments: 'Our mission is to empower creative experimentation across art, science, technology and enterprise for the entirety of Queensland.'[30] He

---

[22] Nevin Martell, 'Meet the Man Who is Turning DC's Library System into a National Model', *The Washington Post* (online), 30 March 2016 <https://www.washingtonpost.com/lifestyle/magazine/meet-the-man-who-is-turning-dcs-library-system-into-a-national-model/2016/03/30/5d06eda0-db50-11e5-891a-4ed04f4213e8_story.html>.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ricky Ribeiro, *Public Libraries Use Technology to Redefine Their Purpose* (27 May 2016) StateTech <http://www.statetechmagazine.com/article/2016/05/public-libraries-use-technology-redefine-their-purpose>.
[27] Scott Grunewald, *The Largest Library in the World Begins 3D Scanning Its Massive Collection of Historical Texts and Artifacts* (25 May 2016) 3DPrint.com <https://3dprint.com/135773/british-library-3d-scanning/>.
[28] Mark Hatch, *The Maker Movement Manifesto: Rules for Innovation in the New World of Crafters, Hackers, and Tinkerers* (McGraw Hill Education, 2014) 172.
[29] Josh Nicholas, *Inside the Library of the Future* (23 December 2015) Business Insider <http://www.businessinsider.com.au/photos-inside-the-library-of-the-future-2015-12>.
[30] Ibid.

observes: 'In an ideal world people would feel inspired, curious, active and engaged with their learnings, but we don't live in an ideal world.'[31]

There have also been efforts to establish makerspaces in regional libraries in Australia.[32] Such regional 3D printing hubs could play a significant role in education, innovation, and technology development.

The digitisation of libraries has raised larger questions about copyright law and the operation of defences, exceptions, and limitations. In two important precedents, United States courts have applied the defence of fair use in respect of digital libraries associated with HathiTrust and Google Books.[33] There remain questions, though, whether Australia's limited defence of fair dealing would extend to mass digitisation of copyright works by cultural institutions.[34]

III GALLERIES

In addition to libraries, galleries have faced copyright issues, particularly in respect of artistic works. In the United States, the Bridgeman Art Gallery could not protect photographic copies of public domain images under copyright law because there was a lack of originality.[35] On occasions, galleries have faced claims in respect of authorising copyright infringement for displaying allegedly infringing works.[36] There have also been conflicts over moral rights and cultural institutions – for instance, in respect of the National Gallery of Australia, and the National Museum of Australia.[37] There have been issues about educational institutions, making false copyright claims over works which

---

[31] Ibid.

[32] Nathalie Fernbach, *Library's Ideas Space Brings Robotics and 3D Technology to Burdekin Region* (2 March 2016) ABC News <http://www.abc.net.au/news/2016-03-02/library-digital-space-keeps-rural-community-switched-on/7214034>.

[33] *Authors Guild v HathiTrust*, 755 F 3d 87 (2nd Cir. 2014); *The Authors Guild v Google Inc.,* 804 F 3d 202 (2nd Cir, 2015).

[34] Australian Law Reform Commission, *Copyright and the Digital Economy*, Report No 122 (February 2014) <http://www.alrc.gov.au/publications/copyright-report-122>.

[35] *Bridgeman Art Library v Corel Corporation*, 25 F Supp 2d 421 (SDNY 1987), modified 36 F Supp 2d 191 (SDNY 1999).

[36] *Théberge v Galerie d'Art du Petit Champlain Inc* [2002] 2 SCR 336; 2002 SCC 34.

[37] Matthew Rimmer, 'Crystal Palaces: Copyright Law And Public Architecture' (2002) 14(2) *Bond Law Review* 320; Matthew Rimmer, 'The Garden of Australian Dreams: The Moral Rights of Landscape Artists' in Fiona MacMillan and Kathy Bowrey (ed), *New Directions in Copyright Law: Volume 3* (Edward Elgar, 2006) 132.

had fallen into the public domain.[38] There has also been discussion about the use of Creative Commons licensing in respect of 3D printing.[39]

In *Digital Handmade*, Lucy Johnston provides a survey of makers and designers who use digital technologies and fabrication techniques to create works of art, craft, jewellery, and fashion.[40] 3D printing has been utilised by the growing maker movement of creators and artists.

In the gallery sector, there has been some interesting experimentation with 3D scanning and 3D printing. The National Gallery of Australia has collaborated with CSIRO in respect of 3D scanning of artwork in the *Myth + Magic: The Art of the Sepik River* exhibition.[41] Six objects on display were scanned and recreated as 3D digital sculptures in a unique collaboration between the NGA and the CSIRO.

Louise Maher noted: 'In the case of the museums and galleries, they have a lot of objects — 3D objects — that have typically been trapped in the physical domain.'[42] Exhibition curator Crispin Howarth said visitors could view the work on touch screens: 'It is a chance for them to look at these artworks before actually discovering the real artworks themselves'.[43]

The copyright regime in respect of galleries needs to be updated in Australia to provide for better digital access.[44]

IV MUSESUMS

Museums have also faced a range of issues with not only copyright law, but also cultural heritage law.[45]

---

[38] Michael Weinberg, *Cultural Institutions Behaving Badly: Stupid Reactions to 3D Scanning* (22 January 2015) Public Knowledge <https://www.publicknowledge.org/news-blog/blogs/cultural-institutions-behaving-badly-stupid-reactions-to-3d-scanning-and-co>.
[39] Jane Park, *Meeting debrief and next steps: the Challenge of Attribution, or 'View Source,' in 3D printing* (15 July 2015) Creative Commons <https://creativecommons.org/2016/07/15/meeting-debrief-next-steps-challenge-attribution-view-source-3d-printing/>.
[40] Lucy Johnston, *Digital Handmade: Craftmanship and the New Digital Revolution* (Thames & Hudson, 2016).
[41] Louise Maher, *CSIRO's 3D Collaboration with the National Galley Virtually Shares Rare Papua New Guinea Tribal Art* (2 October 2015) 666 ABC Canberra <http://www.abc.net.au/news/2015-10-02/csiro-3d-art/6817218>.
[42] Ibid.
[43] Ibid.
[44] Emily Hudson and Andrew Kenyon, 'Digital Access: The Impact of Copyright on Digitisation Practices in Australian Museums, Galleries, Libraries and Archives' (2007) 30(1) *University of New South Wales Law Journal* 12.

In the United States, the Smithsonian was a pioneer in the use of 3D printing for its galleries, museums, and cultural institutions.[46] The Secretary of the Smithsonian, G. Wayne Clough, observed that the Smithsonian website had made available a wide range of data to enable students and researchers to create replicas of cultural objects using 3D printers. He commented: 'Three-dimensional imaging will allow us to take irreplaceable, one-of-a-kind artefacts heretofore seen only in museums and, in a sense, put them in the hands of learners around the world'.[47] The site Smithsonian X 3D has been a website to encourage 3D printing in respect of museum objects.[48] 3D printing of dinosaur bones has been a particularly popular activity at the Smithsonian.[49]

The British Museum has released scans of artefacts to let the public 3D print their own museum pieces at home.[50]

Like their United States and United Kingdom counterparts, Australian museums have experimented with the use of 3D printing. In May 2016, the University of Queensland hosted an exhibition *Real to Relic: Museums in 3D*.[51] Beth Hinds commented: 'Real to Relic aims to show the exciting possibilities of 3D modelling and printing for both museum workers and visitors'.[52] She said: 'Just imagine being able to study an exact replica of a dinosaur bone with no risk of damaging it, or visiting the Louvre from your home in Brisbane.'[53] Beth Hinds observed: '3D technology will impact things like cultural repatriation, virtual exhibitions, and reproducing valuable, vulnerable or destroyed artefacts.'[54]

---

[45] Grischka Petri, 'The Public Domain vs. The Museum: The Limits of Copyright and Reproductions of Two Dimensional Art' (2014) 12(1) *Journal of Conservation and Museum Studies* art 8 <http://www.jcms-journal.com/articles/10.5334/jcms.1021217/>.

[46] G Wayne Clough, *How will 3D Printing Change the Smithsonian?* (February 2014) Smithsonian Magazine (online) <http://www.smithsonianmag.com/ist/?next=/smithsonian-institution/how-will-3d-printing-change-the-smithsonian-180949426/>.

[47] Ibid.

[48] Smithsonian Institution, *Smithsonian X 3D* <http://3d.si.edu/>.

[49] Eric Larson, *Hold a T-Rex-Bone in Your Bare hands, Invites Smithsonian* (11 June 2014) Mashable <http://mashable.com/2014/06/11/3d-printed-dinosaur-bones/#acegYWBEREqD>.

[50] James Vincent, 'British Museum releases scans of artefacts to let you 3D print your own museum at home', *The Independent* (online), 4 November 2014 <http://www.independent.co.uk/life-style/gadgets-and-tech/britishmuseum-releases-scans-of-artefacts-to-letyou-3d-print-your-own-museum-at-home-9837654.html>.

[51] The University of Queensland, *Real to Relic: Museums in 3D* (18 May 2016) <https://www.uq.edu.au/news/article/2016/05/printing-history-museums-come-life-3d>.

[52] Ibid.

[53] Ibid.

[54] Ibid.

The Queensland Museum has been a pioneer in the use of 3D printing in respect of its collection – particularly in respect of its dinosaur exhibits. Archaeologist and Senior curator of the Geosciences Program Dr Scott Hucknull has been a leader in 3D digitising the Queensland Museum from dig site to display.[55] He has emphasized that 3D printing creates new opportunities for research, scientific communication, open-access collections, displays and curation. He has also focused upon how 3D printing and 3D augmented reality could be involved in the monitoring of collections, including preservation practices and repair.

The exhibition *Lost Creatures* sought to use digital technology to display 215 million years of Australian palaeontology.[56] Scott Hucknull explained his interest in the use of digital technology and 3D printing in the context of museums: 'So we are going into the virtual world where we can create these amazing collections of the fossils in really hyper-realistic detail and then share them with the public, whether that's through 3-D printing, through digital animation and modelling, or now in a holographic sense'.[57] Hucknull did qualify his comments: 'Of course we are not necessarily going to do that to a fragile one-of-a-kind fossil, but if we can 3-D print out the exact same replica, then we can do that.'[58] He is concerned that 'the traditional replication process that has been going on for 150 years in museums is a bit detrimental to the fossils themselves'.[59] Hucknull commented: 'So to be able to have a hands-off approach where you can just take a digital camera, create a three-dimensional model of the fossil and then print it out right in front of people's eyes, it's really quite a fascinating process'.[60] Hucknull concluded that 3D printing encouraged a much more interactive experience between the audience and the subject matter of the museums: 'They engage with the fossils and our natural history way more than they would normally staring through some glass.'[61]

The Powerhouse Museum in Sydney has been commissioning and exhibiting 3D printed works of fashion, art and design as part of an exhibition entitled *Out of the Hand: Materialising the Digital*.[62] The curator of the Powerhouse

---

[55] Scott Hucknull, *From Dig to Digital – Breaking the "Rules" of Museums* (15 October 2015) TEDxQUT <https://www.youtube.com/watch?v=heENXNghbrk>.
[56] ABC Radio National, 'Dinosaurs come to life at Queensland Museum thanks to holograms and 3D printing', *The Science Show*, 19 March 2016 (Robyn Williams) <http://www.abc.net.au/radionational/programs/scienceshow/dinosaurs-come-to-life-at-queensland-museum-thanks-to-holograms/7258540>.
[57] Ibid.
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] The Powerhouse Museum, *Out of Hand: Materialising the Digital* (2016)<https://maas.

exhibition, Matthew Connell, observed that 3D printing is allowing designers to experiment: 'It allows for the role of the organic, for biomimicry, to return to design.'[63] He commented: 'We are used to straight, Euclidean shapes, but 3D printing allows us to jump constraint of design.'[64]

While 3D printing dinosaurs may be safely within the public domain, museums will face legal challenges if they engage in 3D scanning and printing of cultural objects, which are still subject to copyright protection. Museums, in particular, would benefit from more expansive copyright exceptions under economic rights dealing with preservation of cultural heritage. Australia's moral rights regime has a general exception in respect of preservation of cultural heritage.

There have been interesting ethical issues arising in respect of 3D printing items of cultural heritage in jeopardy, like works in war-torn Syria.[65]

V ARCHIVES

Archives have also increasingly been a hive of activity in respect of 3D printing, and the maker movement. There has been a Steampunk-driven nostalgia for designs from past technological ages and epochs.

There has also been 3D printing of designs held in Australian archives. In one striking example, the rediscovery of a prosthetic hand design developed in 1845 has inspired the production of a 3D-printed body-powered partial hand prosthesis. [66] US mechanical designer Ivan Owen came across the 19th-century design using the National Library of Australia's online archive, Trove. He found the records of a prosthetic hand developed by Adelaide-based dental surgeon Dr Robert Norman. This enabled Ivan Owen to develop a pulley

---

museum/event/out-of-hand-materialising-the-digital/>; Jessica, *New Kinematics Petals Dress Debuts at Powerhouse Museum* (9 January 2016) Nervous System Blog <http://n-e-r-v-o-u-s.com/blog/?p=7430>; Marcus Strom, 'Australian architect launches revolution with arrival of biggest ever 3D printer', *The Sydney Morning Herald* (online), 4 September 2016 <http://www.smh.com.au/technology/sci-tech/outside-the-box-the-australian-architect-launching-a-3d-printing-revolution-20160901-gr6pni.html>.

[63] Marcus Strom, 'Australian architect launches revolution with arrival of biggest ever 3D printer', *The Sydney Morning Herald* (online), 4 September 2016<http://www.smh.com.au/technology/sci-tech/outside-the-box-the-australian-architect-launching-a-3d-printing-revolution-20160901-gr6pni.html>.

[64] Ibid.

[65] Sarah Bond, 'The Ethics of 3D-Printing Syria's Cultural Heritage', *Forbes* (online), 22 September 2016 <http://www.forbes.com/sites/drsarahbond/2016/09/22/does-nycs-new-3d-printed-palmyra-arch-celebrate-syria-or-just-engage-in-digital-colonialism/#5c6d18972d26>.

[66] Hannah Walmsley with Philip Clark, *World-First 3D-Printed Hand Prosthesis Inspired by 1845 Design Held in Online Archive* (17 December 2015) 666 ABC Canberra <http://www.abc.net.au/news/2015-12-17/world-first-3d-printed-hand-prosthesis-inspired-by-1845-design/7032736>.

mechanism for the design of a contemporary prosthetic hand. Assistant Director-General at the National Library Dr Marie-Louise Ayres commented:

> As a result of international collaboration, more than 1,600 people have received a 3D-printed hand at low cost. Ideas cross over centuries and an item that people might not have thought to be significant was digitised and the right person found it at the right time.[67]

The National Library of Australia and the National Science Centre in Canberra have also collaborated to develop a replica of Ivan Owens' 3D-printed prosthetic hand.

The creation of digital archives have presented a range of copyright issues – particularly in respect of the copyright term, orphan works, and the scope of copyright exceptions.[68] Orphan works – where the author is lost or missing - are an awkward problem for cultural institutions.

VI CONCLUSION

In light of recent developments in respect of 3D printing, there is a good case to be made to update Australia's anachronistic copyright laws, generally, and in respect of cultural institutions, more particularly.

The Australian Law Reform Commission and the Productivity Commission have made some useful recommendations for copyright law reform – paying special attention to the position of libraries, archives, galleries, and museums.[69] Hopefully, the Turnbull Government will pay heed to the recommendations of these policy-makers. The topic of 3D printing certainly highlights a number of doctrinal and policy issues in respect of copyright law. 3D printing poses challenging issues in respect of the crossover between copyright law and designs law. 3D printing highlights the need for a broad, flexible defence of fair use in Australia – like the United States. There is a pressing demand to update the old exceptions for cultural institutions – like libraries, galleries, museums, and archives. The takedown and notice system certainly needs reform and modernisation in the current age of 3D printing. Technological

---

[67] Ibid.

[68] See the unsuccessful challenge to the copyright term extension in the United States by Brewster Kahle of the Internet Archive in *Kahle v Gonzales*, 487 F 3d 697 (9th Cir, 2007).

[69] Australian Law Reform Commission, *Copyright and the Digital Economy*, Report No 122 (February 2014) <http://www.alrc.gov.au/publications/copyright-report-122>; Productivity Commission, *Intellectual Property Arrangements – Draft Report* (April 2016) <http://www.pc.gov.au/inquiries/current/intellectual-property/draft/intellectual-property-draft.pdf>.

protection measures have also proven to be a cumbersome system of uber-copyright. The long term of copyright protection is proving to be troublesome. There is a need for policy solutions for the problem of orphan works. Creative commons licensing, open access, and open innovation could be particularly helpful and useful for cultural institutions.

The full impact of 3D printing on society and the economy remains uncertain. Dr Angela Daly provides a cautionary warning that we do not yet know the full extent of the influence of 3D printing:

> Time will tell how disruptive a technology 3D printing truly is in a socio-legal sense. However, given the political economy of 3D printing's development as a consumer-accessible technology, the involvement of the nation-state and large corporations as well as individuals in its use, it would seem that those who proclaimed 3D printing as a liberatory technology bringing about the end of scarcity and end of control—as with the Internet—have probably done so prematurely.[70]

Nonetheless, 3D printing provides a range of opportunities for cultural industries, manufacturing, information technology, bioprinting, and the provision of health-care. The technology also has a number of important applications for cultural institutions – such as libraries, galleries, museums, and archives. 3D printing provides new opportunities for representing cultural heritage and history. The inclusion of makerspaces and fabspaces will also provide new facilities and utilities for cultural institutions. Libraries, galleries, museums, and archives will hopefully become innovation hubs and creative foundries.

[70] Daly, above n 6, 99.

How Could Technology Improve the Working of Australian Courts?

Anne Wallace*

In an address to a packed audience in Melbourne earlier this year, the British legal technology expert and futurist, Professor Richard Susskind,[1] gave a compelling insight into the way that modern technology is transforming the work of lawyers and courts. He posed this important question:

"Is a court a service or a place?"[2]

What Susskind was suggesting was the former; that rather than conceptualising a court as a physical entity — a registry, a courtroom or court building — we should think of it as a service. That service, in its broadest sense, is the administration of justice, the process by which the courts adjudicate disputes and determine the outcome of criminal cases, by finding facts, interpreting and applying the law.

As the writer has noted elsewhere, over the past three decades Australian courts, along with courts in most of the developed world, have made extensive use of various forms of technology to assist them in their work.[3] In this paper I suggest that shifting the focus to the notion of the court as a service helps us identify several key respects in which technology could be used to further improve their ability to carry out their role. The recent Victorian Royal Commission into Family Violence identified several of these aspects, but they have broader application beyond Victoria and the issue of family violence.

'Improvement' in this context might mean many things. It could mean more efficient delivery of services. In this context, 'efficiency' is usually defined in terms of speed (or its opposite, delay) and the cost of the resources (principally judicial labour) that produce outcomes in court cases.[4] Improvements might be

---

* Professor, School of Business and Law, Edith Cowan University.

[1] See *Richard Susskind* (2016) <http://www.susskind.com/>.

[2] Richard Susskind, 'The Future of Courts & Legal Services' (Speech delivered at the Sir Zelman Cowen Centenary Oration, Victoria University, Melbourne 3 May 2016).

[3] Anne Wallace, 'Courts and their Publics – Technology and the Way Forward' in Australasian Institute of Judicial Administration, *Australian Courts: Serving Democracy and its Publics* (Australasian Institute of Judicial Administration, 2013) 17; Anne Wallace and Roz Macdonald, 'Review of the Extent of Courtroom Technology in Australia' 12(3) *William & Mary Bill of Rights Journal* 649.

[4] This is the approach taken in the annual reports by the Australian Productivity Commission; Productivity Commission, *Report on Government Services 2016 Volume C Justice Chapter 7 Courts* 7.27-7.48 (Commonwealth of Australia, 2016).

aimed at improving the quality of judicial decisions, leading to better outcomes and greater public confidence in the court system. Improvements also might be focussed on improving the experience of court users — litigants, defendants, witnesses, jurors, representatives of the media and members of the public. That experience might include the provision of information to assist them, assistance in accessing and using the court building and its facilities, and their experience in the courtroom (for example, using interpreters). Taking it one step further, technology might be used to develop new ways of delivering court services and administering justice. Focusing on the notion of 'service' rather than 'place' can help identify how technology can serve to enable change, rather than merely reinforce existing practices.

Australian courts and tribunals now employ a wide variety of technologies. These include standard office automation and database tools, local and area networks, registry and case management systems, and various types of more specialised software.[5] The development of the Internet has provided a convenient platform for courts to provide information to the public and other categories of courts users, via their websites.[6] Increasingly, court websites are now serving as electronic 'gateways' to enable individuals to file cases, track the progress of their matters, and to search for and obtain information about case listings.[7] Audio-visual technology has enabled the extension of the boundaries of the courtroom by enabling participation from locations external to the physical space,[8] and a number of courts are now experimenting with the use of social media to assist in their communication with the media, and the public.[9]

Yet, despite this extensive experience, there is evidence that there are still areas of court operations where the technology that is employed is out-dated and of an insufficient quality to deliver the functionality that is required for modern court operations. As a result there is still considerable room for improvement in the administration of justice.

---

[5] Wallace, above n 3, 19-20.

[6] Ibid 21-23.

[7] Ibid 25-27; See for example, Federal Court of Australia, *Online Services* <http://www.fedcourt.gov.au/online-services>; NSW Attorney-General's Department, *NSW Online Registry* <https://onlineregistry.lawlink.nsw.gov.au/content/>.

[8] Emma Rowden et al, *Gateways to justice: design and operational guidelines for remote participation in court proceedings* (University of Western Sydney, 2013) 21-22.

[9] Jane Johnston, 'Communicating justice: a comparison of courts and police use of contemporary media' (2013) 7 *International Journal of Communication* 1667; Jane Johnston, 'Courts' new visibility 2.0' in Patrick Keyzer, Jane Johnston and Mark Pearson (eds), *The Courts and the media: challenges in the era of digital and social media* (Halstead Press, 2012) 41.

This was illustrated dramatically by the findings of the recent Royal Commission into Family Violence in Victoria.[10] While the Commission's work was directed specifically to Victoria, a number of its findings and recommendations in relation to the application of technology in court processes are worthy of consideration in other jurisdictions where courts face similar workload issues and populations of court users with similar needs and concerns.

The Royal Commission found that family violence matters were having a significant impact on the workload of the Magistrates Courts in Victoria and that the courts were struggling to cope.[11] It found that this was, in part, the product of significant structural problems, observing that 'increases in demand have led to chronic infrastructure deficiencies and unsustainable demand on court-based professionals and services.'[12] From the Commission's report, it is clear that technology has a critical role to play in addressing some of these issues.

A key feature of the Commission's report was its focus on the experience of court users, in this case, applicants for family violence intervention orders. Its recommendations for improving the application of technology to court processes illustrate the way that viewing a court as a 'service' rather than a 'place' opens the door to further innovation in the administration of justice. An approach that views a court primarily as a 'place' — a building or room where individuals come to file their cases, have them adjudicated and have justice dispensed — will tend to focus on improvements that enhance the way that cases are currently conducted and that court operations are currently run. A 'service' approach, on the other hand, focuses attention on the nature of the court's role and what is required to fulfil it most effectively, with a view to improving the experience of court users and producing better outcomes.

For example, the Victorian Royal Commission examined the operation of court registries in some detail. This is an area where, as noted above, a great deal of technology has been employed in improving the 'back end' of court operations—registry records, case management and filing, etc. However, as the Royal Commission identified, the current approach to applying technology to court registries Victoria has maintained the focus on the court registry as a physical location.

---

[10] Royal Commission into Family Violence (Victoria), *Royal Commission into Family Violence, Report and Recommendations* (March 2016) <http://www.rcfv.com.au/Report-Recommendations>.
[11] Ibid vol 1, 54, 148 reporting a 34.5% increase in the number of Family Violence Intervention Order applications to the Magistrates Court of Victoria over the four years to 2013-14.
[12] Ibid vol 3, 26.

The Commission found that the outmoded nature of the registry and case management system in the Victorian Magistrates and Childrens Court meant that unnecessary amounts of court time and resources were spent undertaking data entry and manual processing.[13] The fact that court documents were kept in physical, rather than electronic, files also meant that transferring cases between courts was less efficient and more labour intensive.[14]

However, rather than simply recommending an upgrade to the software, the Commission also recommended replacing the current physical court registries with an 'eRegistry' using electronic, rather than physical, case files. Registry services would be centralised and accessed through an online portal (also accessible at any court) and dealt with by a specialised workforce 'to field online and phone queries relating to procedural and filing matters.'[15] As the Commission noted, a number of other Australian jurisdictions have also moved in this direction.[16]

The Commission recommended this approach as a way of freeing up registry staff generally to take on roles that were more directed to supporting court users and magistrates.[17] In family violence matters, the Commission envisaged registrars operating as 'highly skilled and proactive … case managers'[18] engaging directly with court users, answering queries, reviewing files, supporting magistrates and preparing risk assessments and generally managing family violence lists.'[19] This vision is an example of the way in which focussing on the notion of the registry as a 'service' rather than a 'location' can promote innovation, and take improvement one step further.

A focus on a court as a 'place' also tends to promote a view of it as a 'stand alone' institution. In fact, as the Victorian Royal Commission found, courts need to be able to share information with other courts, and agencies. Information technology is a key tool in enabling them to do that efficiently and effectively. The Commission was critical of the limited capacity of existing court information technology systems in Victoria to enable the sharing of information between courts, observing that:

> It is essential for the appropriate adjudication of FVIO [Family Violence Intervention Order] proceedings, and criminal

---

[13] Ibid 152-3, 162.
[14] Ibid 153.
[15] Ibid 163.
[16] See, for example, NSW Attorney-General's Department, *NSW Online Registry* <https://onlineregistry.lawlink.nsw.gov.au/content/>.
[17] Royal Commission into Family Violence (Victoria), vol 3, above n 10, 163.
[18] Ibid 169.
[19] Ibid.

> proceedings involving family violence, that judicial officers are aware of relevant parallel proceedings both within their court, and in other courts across the state and federally.[20]

This is clearly a finding that has implications, not just for Victoria, but also for courts nationally. Australia's jurisdictions currently do not have any systematic process for enabling electronic data exchange between courts in different jurisdictions dealing with related matters, and family violence is only one example of an area of law where there may be related proceedings in different jurisdictions. The need to convey case documentation and information also arises when cases are transferred under cross-vesting procedures, and when they are escalated to different levels of appellate review.

The Victorian Royal Commission also recommended improvements to the Victorian courts' technology platform to enable them to more easily share information with other relevant agencies, accompanied by legislative clarification of privacy requirements.[21] Again, while the Commission's brief was confined to family violence, it is possible to envisage situations in other areas of the law where it may be thought desirable for courts to be able to share information with other government agencies and for them to have access to effective technology that enables that.

The way court listings are currently managed provides another example of the way technology in courts is sometimes focussed more on the court as a 'place' rather than a 'service'. It is common now, in many court buildings, to find large electronic screens near the entrance listing the cases for that day and indicating in which courtrooms they are being heard. These have largely replaced the previous system of pinning a paper notice (generated from the court's computer system) to a noticeboard.

An approach that views the court as a service — the dispensation of justice and the adjudication of disputes — might interrogate the way that cases are currently listed. It might ask whether that approach is providing the best service to court users, and whether technology might be able to assist in providing a better service. The current system of listing cases usually requires parties to present themselves at court at a fixed time, on the basis that their matter may 'called' at any point from that time on. The Victorian Royal Commission found this lack of certainty is a source of added stress for complainants in family violence matters who also, in many courts, have to wait in areas where they are co-located with the alleged perpetrator and that

---

[20] Ibid 163.
[21] Ibid vol 1, ch 7.

person's supporters.[22] A recent review of the operations of the criminal courts in England and Wales also identified concerns about the efficiency of this method of case listing.[23]

The Royal Commission suggested the use of staggered listings, so that matters were listed either in the morning or the afternoon, as one solution to this problem.[24] However, it also noted the potential for technological solutions in the form of 'a real-time airport-style electronic display of listed matters, and alerts transmitted to parties' mobile phones'[25] or issuing court users with electronic devices that transmit a signal when their matter is going ahead, allowing them to remain outside, but nearby, the court.[26]

The Royal Commission suggested that courts could provide greater guidance to parties by developing benchmarks for waiting times for common court processes.[27] It was also concerned about the pressure of the volume of the cases on the courts and recommended capping family violence lists 'at a level that allows magistrates sufficient time to hear each matter.'[28] This would also require benchmarking to establish what is 'sufficient time.'

The Commission pointed out that '[e]ffective use of benchmarks necessitates data-collection practices that allow courts to reliably measure performance.' At a national level, the Australian Productivity Commission has established benchmarks in relation to acceptable levels of backlogs (measured against defined time standards for the disposition of matters)[29] However, a perusal of court annual reports and other published information has not disclosed any instances of courts undertaking benchmarking in relation to other aspects of the court 'service,' such as waiting time, or the amount of time that judicial officers are able to devote to particular categories of cases. Technology, in the form of appropriately designed case management systems, has an obvious role to play in assisting courts to establish benchmarks, and to monitor performance against them.

---

[22] Ibid, 167, 170.
[23] Brian Leveson, *Review of Efficiency in Criminal Proceedings* (Judiciary of England and Wales, January 2015) 142 [146].
[24] Royal Commission into Family Violence (Victoria), above n 10, 167.
[25] Ibid 168.
[26] Ibid.
[27] Ibid.
[28] Ibid 168.
[29] Australian Productivity Commission, above n 4, 7.28.

I CONCLUSION

This brief survey has focussed largely on some of the potential for technology to improve the workings of the courts that were identified in a recent public inquiry in one Australian jurisdiction, in relation to one type of court matter. However, as I have indicated, many of its recommendations resonate more widely across the Australian court system. Improved technology, and improved application of technology, can assist courts to manage their workloads more efficiently, to provide better and more timely information to court staff, judicial officers and court users, and to set and monitor how well they achieve standards of timeliness. These suggestions and recommendations also exemplify Richard Susskind's suggestion that to leverage the maximum benefit to the administration of justice from the public investment in court technology, the focus needs to be on the court as 'a service', rather than a 'place' or an institution.

Choice-of-Court Agreements in Electronic Consumer Contracts in China

Zheng Sophia Tang* and Lu Xu**

I INTRODUCTION

The past a few decades have witnessed the fast-growing development of electronic commercial transactions. Digital buyers worldwide accounted for 24.3% of the world population in 2015. Now nearly 1.8 billion people are engaged in online shopping.[1] E-commerce, by its nature, is cross-border and international. It creates an international virtual market, removing access barriers and costs in traditional commerce. The international nature of e-commerce inevitably raises jurisdictional problems, i.e. since a transaction may have connections with more than one country, which court is competent to decide the dispute if anything goes wrong is in question. E-commerce, unfortunately, challenges traditional jurisdiction rules, which largely depend on geographic connecting factors. One needs to look at the place of contracting, place of performance, the habitual residence/domicile of the parties, etcetera to determine the competent court. Some connecting factors may not always be easy to determine in e-commerce, where contracts are concluded or performed online. Other connecting factors may not be easily predictable by the parties, such as the other party's habitual residence.

Considering the challenges e-commerce has brought to traditional jurisdiction rules, party autonomy is considered the most effective way out in e-commerce. It could avoid the difficulty with identify traditional connecting factors and bring certainty and predictability to the contractual parties. Unfortunately, the appropriateness of party autonomy is questioned in consumer contracts, where the parties have an inequality of bargaining power.[2] The consumers are usually in an unpleasant take-it-or-leave-it position and any choice of court agreement is unilaterally drafted by the business, which generates the possibility of abuse. Jurisdiction in consumer contracts, therefore, is one of the most difficult issues in e-commerce.

---

* Professor, Chair in Law and Commerce, Newcastle University.
** PhD candidate, University of Leeds.

[1] See Statista, *Digital buyer penetration worldwide from 2014 to 2019* (2016) <http://www.statista.com/statistics/261676/digital-buyer-penetration-worldwide/>.

[2] For more comprehensive discussion, see Zheng Sophia Tang, *Electronic Consumer Contracts in the Conflict of Laws* (Hart Publishing, 2nd ed, 2015).

II TWO MODELS

There is no fully satisfactory approach to handle party autonomy in e-consumer contracts internationally. The Hague Choice of Court Convention 2005 intentionally excludes this issue from its scope, given its controversy and the impossibility of reaching a compromise.[3] There are, in general, two major models existing. One is to regulate bargaining power and asymmetric information, represented by the US law; the other is to regulate the effectiveness of a jurisdiction clause, represented by the EU Brussels I Recast.[4] The US law does not provide specific rules to protect consumers in e-commerce. The ordinary rule favouring party autonomy applies, subject to scrutiny of genuine consent.[5] "Genuine consent" is deemed to exist where the business has provided sufficient information, the consumer has opportunities to read, and the consumer has manifested consent in a clear and unambiguous manner.[6] If constructive consent is found, the jurisdiction clause is generally enforceable.[7] It is necessary to note that although e-commerce changes the way of communication, most e-communication meets the criteria if the jurisdiction clause is presented in a readable, clear and durable manner.[8] For example, jurisdiction clauses in click-wrap contracts are held valid as far as the clause is clearly displayed, consumers are given enough time to read, and consumers are required to express their consent unambiguously by clicking on the "Agree" or "Accept" icon. More importantly, the recent development in the US judicial practice shows the gradual relaxation of the standard. For example, the courts have enforced jurisdiction agreements which are displayed in notoriously long contracts only viewable by scrolling down the text;[9] which can only be read by clicking on the hyperlinks;[10] and which are included in browse-wrap contracts and consumers continue to read or access the products.[11]

---

[3] *Convention of 30 June 2005 on Choice of Court Agreements*, concluded 30 June 2005, 44 ILM 1294 (entered into force 1 October 2015) art 2(1)(a).

[4] *Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters* [2012] OJ 351/1 ('*Brussels I Recast*').

[5] *M/S Bremen v Zapata Off–Shore Co (The Bremen)*, 407 US 1 (1972) ('*The Bremen*').

[6] *Specht v Netscape* 306 F 3d 17, 28–32 (2d Cir, 2002); *Serrano v Cablevision* 863 F Supp 2d 157, 164 (EDNY 2012). See also Tang, above n 2, Ch 4, section III.

[7] *The Bremen*, 407 US 1 (1972).

[8] Tang, above n 6.

[9] *Forrest v Verizon Communications*, 805 A 2d 1007, 1010–11 (DC, 2002).

[10] *Person v Google Inc*, 456 F Supp 2d 488, 496–7 (SDNY, 2006).

[11] *Cario v Cross-media Services* (ND Cal, WL 756610, 1 April 2005) slip op 5; *Druyan v Jagger*, 508 F Supp 2d 228, 237 (SDNY 2007).

The EU approach holds jurisdiction agreements in consumer contracts *prima facie* unenforceable, except in limited circumstances.[12] The Brussels I Recast provides the uniform formal validity requirements for jurisdiction clauses, which may be valid if in writing or evidenced in writing, according to common practice between the parties, or pursuant to the commercial custom.[13] It, however, cannot ensure fair bargain or genuine consent. Substantive validity of a jurisdiction clause is subject to the law of the chosen court,[14] which may invalidate the agreement reached by fraud, misrepresentation, or common mistake. However, most domestic laws do not provide rules to protect factual consent of consumers in a standard-form contract. In order to protect consumers in that context, the EU legislators make most jurisdiction clauses unenforceable in consumer contracts, unless they are concluded after disputes have arisen, provide consumers more options, or choose the common domicile of the parties at the time of contracting.[15]

In principle, both models recognise the existence of inequality of bargaining power in consumer contracts, but tackle this by different means. These two models lead to fundamentally different results in protecting consumers and have different economic impacts. It is very clear that the US model may enforce jurisdiction clauses in e-consumer contracts too readily, regardless of the fact that most consumers are unaware of the existence of such a clause or must take efforts to look for and read it. Since e-commerce speeds the contracting process, the overall e-commerce context makes consumers more impatient and unwilling to read. Regulating bargains by traditional standards may no longer be appropriate and sufficient. The EU model recognises such difficulty and, without paying too much attention to regulating online contracting process, it simply denies the enforceability of jurisdiction clauses in consumer contracts.

In terms of economic impact, the US model may be more commercially appealing. It has reduced the commercial risk and cost in engaging in e-commerce. It encourages businesses to enter into the international e-market without being concerned about the potential for unpredictable or inconvenient forums. It is also argued that such a practice may benefit consumers by reduced prices and proliferation of choices.[16] The EU model, therefore, is criticised for maximising commercial risk and forcing businesses to confine

---

[12] *Brussels I Recast*, art 19.
[13] Ibid art 25(1).
[14] Ibid.
[15] Ibid art 19.
[16] *Carnival Cruise Lines, Inc v Shute*, 499 US 585, 595 (1991). RG Bone, 'Party Rulemaking' (2012) 90 *Texas Law Review* 1329, 1364; RA Hillman and JJ Rachlinski, 'Standard-Form Contracting in the Electronic Age' (2002) 77 *New York University Law Review* 429, 439.

their market. It may not only reduce consumers' benefits but also prevent the development of e-commerce to its full potential.[17]

As a result, both approaches need adjustment to meet the requirements of both e-commerce and consumer protection. The US approach may be improved by lifting the standard of sufficient notice, while the EU approach may benefit from a more well defined test that only subjects businesses to the restriction if the businesses have "targeted" the consumer's domicile.[18] Nonetheless, these two approaches have played pioneering roles in the world and provided models for other nations to follow.

III CHINESE APPROACH

The enjoyments brought by e-commerce, most notably the lowering costs and increasing accessibility, have been exploited massively in China, a country where nearly 13% of its retail business is now conducted through online facilities.[19] The 2015 Annual Report of Chinese Online-Shopping Market[20] stated that the market size of general online retail sales has reached an astounding $580 billion, accounting for close to a third of the worldwide figure of $1.67 trillion[21]. China now has over 400 million people as regular digital buyers.[22] In a sense, "online shopping" has become an essential component of life, especially among China's younger generation.[23] More significantly, about a third of the country's e-commerce involves international features, represented by the figure of $809 billion transnational e-commerce of China in 2015.[24] Unfortunately, despite the highly developed e-commerce industry, the Chinese law in regulation of e-commerce is still immature. In particular, the treatment of e-consumer contracts in the private international law of China still largely relies upon the general rules set out for consumer contracts, or just for contracts. Overall, a four-step analysis should be followed. Firstly, a jurisdiction agreement in an e-contract should satisfy some general formal requirements. Additionally, the designated court should also have "substantial

---

[17] For more discussion and counter arguments, see Tang, above n 2, Ch 12, section I.
[18] *Brussels I Recast,* art 17.
[19] China Electronic Commerce Research Centre (CECRC), *2015 Annual Report of Chinese E-commerce Market Statistics* <http://www.100ec.cn/zt//2015ndbg/>.
[20] China Internet Network Information Centre (CINIC), *Report of China Internet Network Information Centre (CINIC)* (June 2016) <http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/dzswbg/201606/P020160622616579052961.pdf>.
[21] Statista, *Retail e-commerce sales worldwide from 2014 to 2019* (2016) <http://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/>.
[22] CNNIC, *The 37th Report of Internet Development in China* (2016), 1 <http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/201601/P020160122469130059846.pdf>.
[23] Ibid 42.
[24] CECRC, above n 19.

connection" with the dispute. Thirdly, it is required that consumers should receive "reasonable notice" with regards to a jurisdiction clause incorporated into a standard form contract.[25] Fourthly, the substantive effectiveness of a choice-of-court agreement will also be examined, especially for a clause in favour of a foreign court.[26] The first three steps aim at regulating the bargaining power of online business by imposing extra responsibilities on the incorporation of such a clause. The final step, on the other hand, attempts to introduce ex-post control over a jurisdiction clause by examining its actual effects on behalf of consumers.

A REGULATING BARGAINING POWER

In terms of regulating bargains, the Chinese law requires jurisdiction clauses to be in writing, which may include any electronic means, including electronic text, telegram, telex, facsimile, electronic data interchange and e-mail.[27] This is a general requirement for all jurisdiction clauses and does not involve any specific concern in balancing the bargaining power in consumer contracts.

The chosen court must have "substantive connections" with the dispute,[28] which may be that the court is located in the domicile of either party, place of contracting, place of performance, location of the subject, place of tort committed, etcetera.[29] In an online sales contract, if the subject is delivered by way of internet information transmission, the domicile of consumers should be considered as the "place of performance"; if the subject is delivered by other means, the place where the delivery is received will be regarded as the "place of performance", unless parties agree otherwise.[30] The substantive connection requirement might prove useful by preventing an e-company from abusing its bargaining power by unilaterally choosing a remote jurisdiction that has no connection to the dispute to create barriers to consumers. However, most businesses would only make a bona fide choice of the court of their domicile, which equally proves inconvenient for foreign consumers and may effectively hamper consumers' access to court.

---

[25] *Judicial Interpretation of The Law on Civil Procedure of The Supreme People's Court* (People's Republic of China) Supreme People's Court, 4 February 2015, art 31 ('*Interpretation*').

[26] According to art 522 of *Interpretation*, a choice-of-court agreement in favour of a foreign court may be declined by Chinese court.

[27] *Contract Law of the People's Republic of China* (People's Republic of China) National People's Congress, 15 March 1999, art 11 ('PRC Contract Law').

[28] *Civil Procedure Law of the People's Republic of China* (People's Republic of China) National People's Congress, 9 April 1991, art 34; *Interpretation*, art 531.

[29] *Interpretation*, art 531.

[30] *Interpretation*, art 20.

The most relevant prerequisite is the latest development provided by the Supreme People's Court in 2015, which states that the choice of court agreement is invalid if the suppliers fail to bring it to the attention of consumers in a reasonable manner.[31] The "reasonable notice" test imposes reasonable duties to the business and ensures sufficient steps have been taken to bring consumers' attention to the jurisdiction clause to prove constructive knowledge and consent. However, no clear guidance has been provided to the "reasonable notice" test. Some recent cases show the test of "reasonable notice" is applied to a large extent by judicial discretion. The existing judicial practice indicates the criteria as follows. Firstly, extra steps usually should be taken by online business providers to bring the attention of consumers to the particular existence of a choice-of-court agreement, apart from other terms in the contract. This usually involves the choice-of-court agreement being written in a noticeable form, such as in bold, or in a different colour. For example, in *Liao Yandong v Tencent*,[32] the court considered a choice-of-forum clause written in bold as sufficient notice in an online service contract. Additionally, if the choice-of-court clause automatically pops out before consumers clicking the "I agree" icon or access to the online service, it is likely for a court to acknowledge the existence of reasonable notice. However, it is uncertain whether a jurisdiction clause included in an online contract without being highlighted specifically will fail the "reasonable notice" test. If an e-contract is clearly readable, is a reasonable length, and requires the consumer to read carefully before clicking to accept, it is unreasonable to argue consumers do not have "reasonable notice" of the existence of a jurisdiction clause. On the other hand, a too relaxed requirement as the sufficient notice in the US law may make the threshold too low and cannot provide sufficient protection to consumers.

Secondly, the court will take into account the duration of the parties' relationship. If the consumer contracts with the same e-business repeatedly for a long time and is presented the same contract containing the jurisdiction clause, the reasonable notice would likely exist. In *Daizhibai v Hangzhou Leihuo Science & Technology Ltd,*[33] where the consumer played an online game operated by the defendant for several years and the service agreement appeared every time when the consumer logged onto the system, the court concluded that the consumer should have plenty chance to read the terms carefully given the length of the performance of the contract,.

---

[31] *Interpretation*, art 31.
[32] Foshan Intermediate People's Court of Guangdong Province, No 06646, 24 May 2016.
[33] Lianyungang Intermediate People's Court of Jiangsu Province, No 00129, 18 January 2016.

Thirdly, if the choice-of-court clause is not displayed directly in the general terms but is only accessible through a hyperlink, the positions of the courts are nevertheless inconsistent. This is clearly indicated in two cases, both concerning the choice-of-forum clause included in the hyperlink, written in bold and underlined, and choosing the jurisdiction of the business's domicile. In *Li Junbo & Zheng Juqi v Tmall Internet Ltd*,[34] the court recognised the validity of a choice-of-forum agreement on the ground that it was shown in a noticeable form and was clearly constructed.[35] In *Cui Haibin v Taobao Internet Ltd,*[36] the same choice-of-forum agreement was held to be invalid for two reasons. Firstly, the full agreement was lengthy, loaded with information and written in a small size. Secondly, there was also one provision allowing the e-business to make unilateral modifications to the terms at any time; and under such circumstances, the updated terms could only be accessed through several steps of operations initiated by consumers. If the choice-of-court agreement is valid, it "significantly increases the cost for consumers to access to redress" and results in imbalance in the parties' rights and obligations to the detriment of the consumers. The jurisdiction clause was held invalid. It shows the more onerous and unusual the clause is, the more steps should be taken to bring consumers' attention to the jurisdiction clause and the more easily accessible the clause must be.[37] Including an onerous jurisdiction clause in a hyperlink, therefore, will be held invalid.

B EFFECTIVENESS OF JURISDICTION CLAUSES

Chinese law does not hold jurisdiction clauses in consumer contracts *prima facie* unenforceable, as the EU Brussels Recast Regulation has done. The control of substantive effectiveness of jurisdictional clauses is stated as a general principle of all standard consumer contracts, requiring that a clause should not impose unfair or unreasonable burdens on behalf of consumers.[38] In terms of jurisdiction clauses, it requires that consumers should not be deprived of fair and reasonable access to courts.

The issues are sometimes addressed in court by applying the "reasonable notice" test that involves the consideration of both formal requirements and substantive effects of a jurisdiction clause in determining the standard of

---

[34] Hanjiang Intermedium People's Court of Hubei Province, No 96/24, 28 June 2016.
[35] The court did not provide further explanation of what it meant by "clear construction".
[36] Taizhou Intermedium People's Court of Jiangsu Province, No 12/12421 June 2016.
[37] cf PRC Contract Law, art 40.
[38] *Law of the People's Republic of China on Protection of Consumer Rights and Interests* (People's Republic of China) National People's Congress, 31 October 1993, art 24; *Administrative Measures of Online Trading* (People's Republic of China) State Administration for Industry and Commerce, Order No 60, 26 January 2014, art 17.

"reasonableness" in a specific case. In some cases, the Chinese courts may not provide full effectiveness to a jurisdiction clause, which, however, is not due to the consideration of administration of justice or consumer protection, but due to a zealous attempt to protect the jurisdiction of Chinese courts, especially concerning the effectiveness of a jurisdiction clause choosing a foreign court. The law does not expressly require the Chinese courts to decline jurisdiction if the foreign court is chosen in an exclusive jurisdiction clause. Therefore, some Chinese courts may decide to exercise jurisdiction anyway, irrespective of a valid jurisdiction clause choosing a foreign court.[39] This may nevertheless benefit Chinese consumers, who would avoid the consequence of having to sue a foreign company abroad. However, other courts may wish to enforce a foreign jurisdiction clause anyway. The uncertainty of the effectiveness of a foreign choice-of-court clause cannot be relied on in protecting Chinese consumers. A Chinese court, on the other hand, cannot decline exercising jurisdiction if it is chosen in a jurisdiction clause, even if it requires a foreign consumer to sue in China and the dispute may have no substantive connections with China.[40] It may largely benefit Chinese businesses, which could confidently insert a clause in e-contracts choosing Chinese courts and such clauses would be enforced by Chinese courts given the "reasonable notice" test is satisfied.

C COMPARATIVE STUDY

In general, the Chinese law follows the US model. Although the EU model may provide stronger protection to consumers, the potential cost and burden for businesses are not favoured by Chinese legislators. E-consumers are protected in China through regulating the bargaining power. The newly developed "reasonable notice" test plays a crucial role in determining the success of the Chinese approach. However, there is no consistent guidance provided to apply the test in e-commerce. Since e-commerce changes the communication method, the judges would exercise discretion to determine whether reasonable notice is given on a case-to-case basis. Difficulties usually arise concerning jurisdiction clauses which are included at the end of a lengthy contract which can only be read by scrolling down the bar, which are displayed in small font, in grey colour or against a low contrast background, which are contained in a hyperlink, which are made binding when consumers continue to browse the website, or which are concluded when an icon not expressly stating "Acceptance" is clicked. Furthermore, the approach following the US path

---

[39] *NKK (Japan) v Beijing Zhuangsheng*, Beijing Municipal High People's Court, No 919, 2008; *RNO v Beijing International Music Festival Society*, Beijing Municipal No 2 Intermediate People's Court, No 928, 2004. ZS Tang, 'Effectiveness of Exclusive Jurisdiction Clauses in the Chinese Courts' (2012) 61 *International and Comparative Law Quarterly* 459, 473-476.

[40] *Interpretation*, art 522.

may reduce business risks but does not provide enough protection to consumers. This weakness can be addressed by increase the criteria for the "reasonable notice" test. In other words, the very liberal US approach is inappropriate and the Chinese courts should adopt the higher threshold for "reasonable notice" to be established. This tendency is already shown in the existing court decisions, but given the lack of experience of discretion exercising, a clear guidance, taking the development of technology into account, is necessary to provide certainty and a reasonable standard of protection for consumers.

IV CONCLUSION

Electronic commerce is a significant "sunrise industry" in China. The high profitability of business and wide accessibility for the general public can guarantee its prospective fast growth in the years to come. Doing business in an online environment intensifies the strain between law and technology, and it becomes more obvious when it comes to consumer protection. The protection of consumers as weaker parties, the protection of local business, and the need to continue boosting technology, are the values to balance. Generally speaking, the protection of local business and the need of safeguarding jurisdiction of Chinese courts are central concerns underlining the current legislative framework. On the one hand, the lack of consumer-favourable jurisdictional rules, together with a lenient approach to determining the effectiveness of a choice-of-court agreement, indicate that Chinese law prioritises the protection of local exporting e-business, which constitutes a significantly larger component in the transnational e-commerce of China.[41] A large number of Chinese e-businesses therefore acquire great certainty and predictability in imposing jurisdiction agreements favouring Chinese courts on prospective consumers. On the other hand, the jurisdiction of Chinese courts is secured not only by enforcing clauses choosing local forums, but also through negative attitudes towards foreign-forum selection clauses. It at the same time extends protection towards local e-consumers purchasing imported goods, although they may face risks of accepting jurisdiction in a foreign forum. As a result, Chinese e-commerce has enjoyed a rapid growth in recent years under such a favourable policy and is able to make a noticeable contribution towards domestic economy.

However, an attitude of local-protectionism may not work in the long run. Local exporting e-businesses may experience difficulties when expanding their business overseas. Consumers need confidence to purchase online, without

[41] CECRC, above n 19. Exporting business accounts for 83.2% of total cross-border e-commerce, compared to the 16.8% of importing business.

worrying about the consequence of being deprived of the right of access to justice. Without protection of the appropriate level, consumers may be held back from engaging in e-commerce, thus leaving foreign consumers hesitating to purchase from Chinese exporting businesses due to the lack of proper consumer protection rules.

Under the current legal framework, the protection to consumers can only be provided through a proper interpretation of the "reasonable notice" test in the e-commerce context, before any substantial changes are brought in revising legislation. The introduction of the "reasonable notice" test is to safeguard the genuine consent of parties in agreeing upon a standard contractual clause. To such end, the application of the test should operate on two aspects. Formally speaking, a valid clause should be incorporated in a "reasonable" manner, which involves the examination of noticeable form, clear construction of the clause, and the appropriate steps taken to bring it to the attention of consumers. Substantively speaking, the standard of satisfying "reasonable" notice should be decided by considering the relevant circumstances of the case and the content of the clause. The more onerous and unusual a clause appears, the higher the standard should be. In this regard, the "reasonable notice" test should be put in context with the examination of the "substantive effectiveness" of a jurisdiction clause. Finally, "the substantial connection" requirement should be used to complement the "reasonable notice" test, in order to maintain the minimum link between the chosen forum and the present case.

Overall, at this stage, the guided cases released by Supreme People's Court may be the most effective way to bring uniformity and certainty into current Chinese law to improve the level of consumer protection in internet jurisdiction rules. Future legislation should aim at building a systematic structure which puts together the regulation for online operators, clarified standards of consumer protection and protective jurisdictional rules in a consistent manner.

Myriad in Australia: A Patent U-turn in the right direction?

Elizabeth Siew-Kuan Ng*

I INTRODUCTION

The rapid advancement in new technologies continues to pose immense challenges to the patent system, particularly at the interface between law and biotechnology. In the nascent field of human gene patenting, much academic discourse has been generated on issues relating to patenting of the Code of Life. This subject-matter has divided proponents and opponents to gene patents along the lines of ethics, policy and even self- and national interests. Opponents to patents on human genes portend that the grant of patent rights on the Code of Life (or part thereof) may be akin to a modern day construction of the Tower of Babel. They argue that the grant of patents over an inherent and natural part of a human being is intuitively, ethically and morally repugnant. Others view gene patenting, not as a moral quandary, but fear that the grant of gene patents may impede further research and development and hinder genetic advancement in this promising field. Still others express concern that it may adversely impact on public health and patients' right of access to healthcare services. Proponents of gene patents, on the other hand, rely inter alia on the incentive theory which is fundamental to the patent system. They contend that patents are critical to incentivising and promoting scientific and technological progress which leads to the creation of useful inventions which are beneficial to mankind.

Against this backdrop of competing and often conflicting interests, it is unsurprising that there is no global consensus on the issue of whether human genes are patent-eligible subject-matter. Nonetheless, in an earlier work[1] this author discerned a potential convergence in the US and Indian approaches on certain aspects of gene patenting - that isolated genomic DNA (gDNA) is not patent-eligible subject matter. The author had argued that this represents a

---

* Deputy Chairwoman and Director (Intellectual Property Research Unit), Centre for Law and Business; Director, Graduate Certificate of Intellectual Property program (GCIP); Associate Professor of Law, Faculty of Law, National University of Singapore; LL.B (Hons) University of London; LL.M (First Class) University of Cambridge; Barrister-at-Law (Middle Temple, London); Advocate & Solicitor (Singapore). My thanks to Wan Qing Ng, Yihang Ng and Estella Low for excellent research assistance. The views expressed and any errors are those of the author.

[1] Elizabeth Siew-Kuan Ng, 'Patenting Human Genes: Wherein lies the Balance between Private Rights and Public Access in India and the United States?' (2015) 11 *Indian Journal of Law and Technology* 1.

reasonable departure from the current international practices and is the better approach.[2] It represents an appropriate balance between granting private rights without jeopardising public access. Since then, the 2015 Australian High Court's decision of *D'Arcy v Myriad Genetics Inc & Anor*[3] ("*Myriad Australia*") has fortified the views of this author, at least with respect to naturally-occurring and isolated gDNA.

Building on the author's previous work,[4] this article will focus on the Australian approach to human gene patenting, including references to the US position where relevant. It will present and re-affirm the author's earlier viewpoint that differences in the cultural, economic, technological and patent law developments "are not necessarily inimical to the prospect of adopting a common approach on certain facets of patent law, such as, those relating to the patent-eligibility of isolated genes."[5] The article concludes by presenting that the current approach in Australia is largely consistent with the better approach adopted in the US and India – it represents a U-turn in the right direction.

II SCIENCE OF GENETICS: A BRIEF INTRODUCTION[6]

Since Friedrich Miescher identified DNA as a distinct molecule and his successful isolation of "nuclein" (DNA with associated protein) in 1869,[7] it has taken nearly 150 years for DNA to "[rise] from being an obscure molecule with presumed accessory or structural functions inside the nucleus" to become the "icon of modern bioscience"[8] and probably one of the most hotly contested subject-matter in patent law globally.
Comprising of approximately 20,000-25,000[9] genes within 23 pairs of chromosomes, the human genome forms the "basis of human inheritance".[10]

---

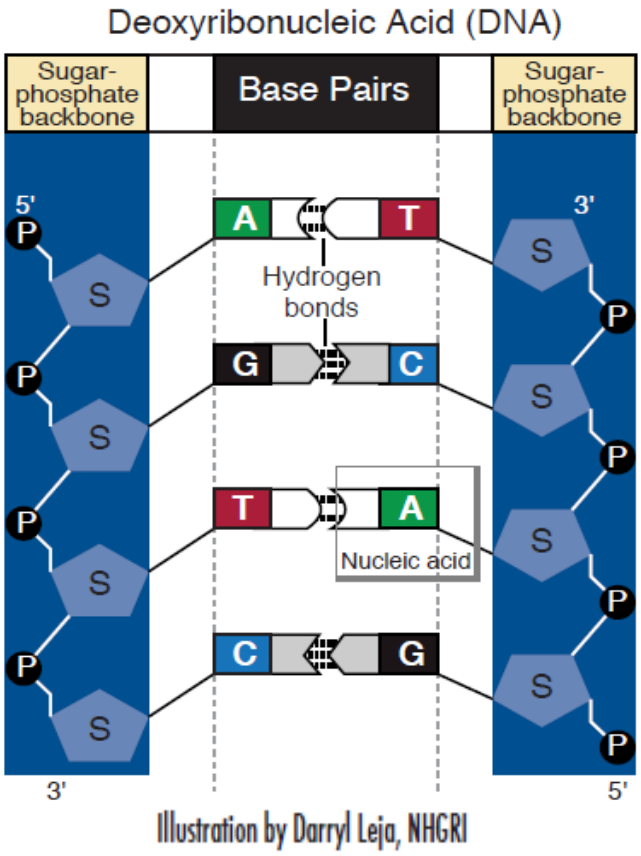
[2] Ibid.
[3] *D'Arcy v Myriad Genetics Inc & Anor* [2015] HCA 35 (7 October 2015).
[4] See Ng, above n 1.
[5] Ibid 4-5.
[6] This brief introduction to genetics is based on the author's earlier article on Patenting Human genes, see ibid.
[7] DNA from the beginning, *DNA and proteins are key molecules of the cell nucleus* (2011) <http://www.dnaftb.org/15/bio.html>; Ralf Dahm, 'Friedrich Miescher and the discovery of DNA' (2005) 278 *Developmental Biology* 274.
[8] Dahm, above n 7, 274.
[9] *AMP v Myriad*, 569 U.S. ___ (2013), Docket No. 12-398; *AMP v Myriad*, 689 F 3d 1303 (Fed Cir, 2012). See also Human Genome Project Information Archive 1990-2003, *About the Human Genome Project* (11 February 2015) <http://web.ornl.gov/sci/techresources/Human_Genome/project/index.shtml>; Genetics Home Reference, *What is a gene?* (30 August 2016) <https://ghr.nlm.nih.gov/primer/basics/gene>.
[10] *AMP v Myriad*, 689 F.3d 1303, 1310 (2012).

Genes form the basic units of heredity in all living organisms. Each gene is made up of DNA and its size varies from a "few hundred DNA bases to more than 2 million bases."[11] DNA controls nearly every aspect of a living organism's physiology.[12] The DNA that is naturally occurring in a cell is referred to as "native" or "genomic" DNA. Its basic structure comprises two strands of nucleotides bound and twisted to form a double helix connected by "cross-bars". There are four standard nucleotides consisting of adenine (A), thymine (T), cytosine (C) and guanine (G) which are chemically paired so that "A" will always bind with "T", and "C" will always bind with "G". (See figure below). The predictable pairings of nucleotides make it possible to deduce its corresponding nucleotide sequence. The precise sequence of a DNA nucleotide generates the essential information that is necessary to build the proteins encoded by a given gene. This process involves DNA being converted to mRNA which is then translated to amino acids which then form proteins. This is known as the central dogma of molecular biology conversion.[13] Whilst some sections of a gene's nucleotide sequence may encode for amino acids, the rest may comprise non-coding and regulatory sequences. The amino acid-coding nucleotide sequences are known as "exons" and the remaining non-coding nucleotides sequences are known as "introns". Typically, a DNA sequence would contain both "exons" and "introns".

DNA can be extracted from its natural cellular environment. The DNA that is extracted in this manner is generally referred to as "isolated gDNA" if the genetic sequence does not undergo any modification. Where the isolated DNA has been modified, typically through splicing and removal of the non-coding introns, the resultant DNA sequence made up of only exons is known as complementary DNA (cDNA). cDNA generally arises from reverse transcription of mRNA, a mechanism that requires human intervention. It may also be synthesised artificially using the mRNA which has already been spliced naturally in the cell such that the introns are removed and only the exons remain. Additionally, there are also *naturally occurring* short exon-only DNA sequences that exist in nature.

---

[11] See Human Genome Project Information Archive 1990-2003, *Human Genome Project* (25 July 2016) <http://web.ornl.gov/sci/techresources/Human_Genome/index.shtml>.
[12] Brief for the United States as amicus curiae in the *AMP v Myriad*, 569 U.S. ___ (2013), Docket No. 12-398.
[13] Scitable, *The Elaboration of the Central Dogma* (17 January 2014) <http://www.nature.com/scitable/ebooks/cntNm-16553173>.



With this brief scientific background in mind, we will proceed to analyse the patent law issues.

III ARE HUMAN GENES PATENT-ELIGIBLE? WHY DOES IT MATTER?

At the outset, three caveats should be highlighted.[14] First, it should be emphasised that whilst issues relating to ethics and morality are important, these concerns have been adequately discussed elsewhere and will not be debated here.[15] Second, this article is not concerned with method patent claims, such as, those relating to genetic testing and diagnostic medicine.[16]

---

[14] See also Ng, above n 1.

[15] See, for example, Elizabeth Siew-Kuan Ng, 'Immoral inventions: Interaction between ethics and biotechnology patent law" (2010) *Singapore Academy of Law Journal* 931; NV Rangantha, *Patenting Human Genes: Moral and Ethical Issues* (2012) Preservearticles <http://www.preservearticles.com/2011120618179/patenting-of-human-genes-moral-and-ethical-issues.html>.

[16] See, for example, *Mayo Collaborative Servs v Prometheus Labs Inc.*, 566 U.S. ___ (2012), Docket No. 10-1150 ("*Mayo*"). This decision was handed down one year before *Myriad*. For an excellent discussion, see Arti K Rai, 'Diagnostic patents at the Supreme Court' (2014) 18(1) *Marquette Intellectual Property Law Review* 1.

Third, the focal point of discussion in this work relates to whether human genes, namely (a) naturally occurring DNA, (b) isolated genomic DNA and (c) cDNA, are patent-eligible subject matter in Australia. Reference to the US approach will also be included where relevant. It is important to note that this patent subject-matter eligibility analysis is merely one of several criteria that must be fulfilled in determining whether an invention can be patentable. To put it another way, even if a particular gene sequence crosses this first hurdle of patent-eligible subject-matter, it would still need to satisfy the other well-established attributes of patentability, such as novelty (new in the light of the prior art), inventive step (non-obvious to the skilled addressee) and industrial applicability (utility).[17]

The question of whether human genes are patent-eligible subject matter was answered in the US by the landmark 2013 US Supreme Court decision in *Association for Molecular Pathology v Myriad Genetics* (*"Myriad US"*).[18] With remarkable unanimity, the nine justices ruled that isolated genomic DNA ("gDNA"), being "products of nature", are not patent-eligible unlike man-made complementary DNA ("cDNA") which do not exist naturally. Until this 2013 US decision, the position adopted by the the patent regimes of many jurisdictions in the developed world, including Australia, was to treat isolated gDNA as patent-eligible subject-matter.[19]

Then in the 2015 ground-breaking *Myriad Australia* decision, the High Court of Australia adopted a broadly similar approach to the US Supreme Court and ruled against the patent-eligibility of human DNA thereby departing from its long-standing national practice, as well as the international trend on human genes patenting.

IV MYRIAD IN AUSTRALIA

On 7 October 2015, the High Court of Australia ("High Court") unanimously held in *Myriad Australia* that an isolated gDNA was not a "patentable invention" as it did not fall under the concept of "manner of manufacture" within the meaning of section 6 of the *Statute of Monopolies* as provided in

---

[17] These are the well-established patentability criteria set out in the Agreement on Trade-Related Aspects of Intellectual Property Rights: see *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1867 UNTS 299, ILM 1997 (entered into force 1 January 1995) annex 1C (*Agreement on Trade-Related Aspects of Intellectual Property Rights*).

[18] 569 U.S. ___ (2013), Docket No. 12-398.

[19] See, for example, E Richard Gold and Julia Carbone, 'Myriad Genetics: In the Eye of the Policy Storm' (2010) 12 *Genetics in Medicine* S39; Matthew Rimmer, 'The Empire of Cancer: Gene Patents and Cancer Voices' (2012-2013) 22(2) *Journal of Law, Information and Science* 18.

section 18(1)(a) of the *Patents Act 1990* (Cth) ("Australian PA"). In coming to its decision, the High Court overturned the decision of the Full Court of the Federal Court of Australia ("Full Court") which had held that the invention was a "manner of manufacture". The Full Court had found that the claimed isolated DNA was chemically, structurally and functionally different from DNA inside a human cell – it resulted in an "artificially created state of affairs for economic benefit" in accordance with the principles set out in an earlier leading High Court of Australia decision of *National Research Development Corporation v Commissioner of Patents*[20] ("*NRDC*").

A WHAT CONSTITUTES "MANNER OF MANUFACTURE"?

The High Court reviewed the existing principle enunciated in *NRDC* on the characterisation of an invention as a "manner of manufacture", namely:

1. Whether the invention as claimed is for a product made, or a process producing an outcome as a result of human action.
2. Whether the invention as claimed has economic utility.[21]

Importantly, the Court held that in claims involving 'a significant new application or extension of the concept of "manner of manufacture"', such as those relating to human genes, apart from the two factors enunciated in *NRDC* above, there are other considerations which the Court should take into account, particularly the purpose of the Australian patent legislation. The High Court elaborated on these additional factors, such as:

> 3. Whether patentability would be consistent with the purposes of the Act and, in particular:
>
> 3.1. whether the invention as claimed, if patentable under s 18(1)(a), could give rise to a large new field of monopoly protection with potentially negative effects on innovation;
>
> 3.2. whether the invention as claimed, if patentable under s 18(1)(a), could, because of the content of the claims, have a chilling effect on activities beyond those formally the subject of the exclusive rights granted to the patentee;
>
> 3.3. whether to accord patentability to the invention as claimed would involve the court in assessing important and conflicting public and private interests and purposes.
>
> 4. Whether to accord patentability to the invention as claimed would enhance or detract from the coherence of the law relating to inherent patentability.

---

[20] (1959) 102 CLR 252.

[21] *Myriad Australia* [2015] HCA 35 (7 October 2015) [28].

> 5. Relevantly to Australia's place in the international community of nations:
>
> 5.1. Australia's obligations under international law;
>
> 5.2. the patent laws of other countries.
>
> 6. Whether to accord patentability to the class of invention as claimed would involve law-making of a kind which should be done by the legislature.

Factors 3, 4 and 6 are of primary importance. Those primary factors are not mutually exclusive … They are nevertheless also relevant to the ongoing development of the concept of "manner of manufacture".[22]

B ARE HUMAN GENES WITHIN THE CONCEPT "MANNER OF MANUFACTURE"?

Applying the *NRDC* principles, the High Court opined that under section 6 of the *Statute of Monopolies*, an invention is something which must reside in something – a product or a process – it must involve "making". It may be an "artificially created state of affairs". In other words, "it must be something brought about by human action[23]."[24] Looking at the claimed invention at hand, the High Court acknowledged that it might in a "formal sense" be said to be a product of human action, nonetheless the essential element of the claimed invention resided in the existence of the information stored in the nucleotide sequences. In other words, whilst the claimed invention might have been formulated as a product, the substance of the claim is actually the information that is embodied in the nucleotide arrangements. This information is discerned, not "made by human action".[25]

Significantly, the High Court went beyond the *NRDC* factors to consider the additional factors enunciated above. The Court concluded that to attribute patentability to the invention as claimed would involve an extension of the concept of 'manner of manufacture' which was not appropriate for judicial determination, nor will it contribute to "coherence in the law". [26] Moreover, such an extension was not supported by Australia's international obligations or the patent laws of other jurisdictions.

---

[22] Ibid.

[23] (1959) 102 CLR 252, 276–277.

[24] *Myriad Australia* [2015] HCA 35 (7 October 2015) [6].

[25] Ibid.

[26] Ibid [94].

C SOME THOUGHTS ON THE AUSTRALIAN APPROACH

Notwithstanding differences in the patent law concepts in the US and Australia (e.g. the Australian concept of "manner of manufacture" is absent in US law), the emerging patent jurisprudence in both countries seem to be potentially converging at least on the issue of patent-eligibility of isolated gDNA (and naturally occurring DNA). Both the US Supreme Court and the High Court of Australia interpreted the claimed invention as essentially claims in respect of the "information stored in the relevant sequences" rather than chemical compounds. In doing so, the central issue was whether the genetic information which forms an essential integer of the claimed invention was patent-eligible. Both Courts held that it was not and denied patent-eligibility to isolated gDNA albeit on different bases. The Supreme Court held *inter alia* that isolated gDNA fell within the "law of nature" exclusion under the US patent jurisprudence – that Myriad had not created or altered the *genetic information* encoded in the BRCA genes. The High Court, on the other hand, grounded its decision on the fact that the claimed invention was not a "manner of manufacture" under the Australian PA. The Court held *inter alia* that the substance of the claim, being the information embodied in the nucleotide arrangements, was not "made by human action".

Importantly, the High Court had rightly considered that claims relating to genetic information lie at the boundaries of what constitutes an invention or a "manner of manufacture", requiring a deliberation of countervailing factors beyond those enunciated in *NRDC*. In the authoritative words of the Court:

> When proper regard is paid to their emphasis on genetic information, the subject matter of the claims lies at the boundaries of the concept of "manner of manufacture". That it does lie at the boundaries is further evidenced by the odd consequence that if the claims are properly the subject of a patent, the patent could be infringed without the infringer being aware of that fact. That consequence coupled with the very large, indeed unquantified size of the relevant class of isolated nucleic acids, all of which bear the requisite information, raises the risk of a chilling effect upon legitimate innovative activity outside the formal boundaries of the monopoly and risks creating a penumbral de facto monopoly impeding the activities of legitimate improvers and inventors[27].[28]

[27] See also the reasons of Gordon J at [259]–[264] where Her Honour discusses the consequences of inhibiting researchers and medical practitioners isolating and testing the BRCA1 gene for other unrelated purposes if the claims are valid.

Likewise, the US Supreme Court in its deliberation was also cognisant of the broader upstream and downstream implications of such patent claims. Notably, its potential deterring effect upon the innovative activities of legitimate improvers and inventors which may hinder future innovation.

Whilst the issue pertaining to the patent-eligibility of isolated gDNA seems settled in both jurisdictions, the position in respect of cDNA appears to be less clear in Australia. Unlike the US Supreme Court which had held that a man-made exon-only cDNA was not naturally occurring and was therefore patent-eligible subject-matter, the High Court of Australia's stance seems less certain. The widely accepted view that the High Court has adopted a broad exclusion by considering cDNA to be patent-ineligible in Australia, is not without detractors.[29] Be that as it may, following the High Court's decision, the Australian Patent Office seems to have adopted a qualified view towards the patent-eligibility of cDNA. Whilst it had originally proposed a blanket ban on the patenting of cDNA, its current position is that cDNA is excluded from patent-eligibility where it "merely replicates the genetic information of a naturally occurring organism".[30] It remains uncertain as to whether a claim that is properly construed as defining a cDNA molecule (rather than information) will be tenable.

V WHY DOES IT MATTER?

Apart from the legal ramifications, perhaps more importantly the issues surrounding the patenting of human genes presents immense upstream and downstream challenges.[31] Since mutations of genes are correlated to diseases, the Courts' responses to the issues pertaining to human gene patenting will impact on gene therapy and medical genetic testing among others. Let's look at the BRCA gene as an illustration.

The BRCA 1 gene codes for the production of the BRCA 1 protein. It is a tumour suppressor gene which acts to repair damage to DNA. Mutation of this gene increases the risk of cancer occurrence. If a genetic test identifies an

---

[28] *Myriad Australia* [2015] HCA 35 (7 October 2015) [93].

[29] See for example, Tom Gumley, *What did the Australian High Court actually say about the patent eligibility of cDNA?* (19 October 2015) Lexology <http://www.lexology.com/library/detail.aspx?g=45b81470-808d-48d4-bed7-7b1e15f928e1>.

[30] Australian Patent Office, *Examination practice following the High Court decision in D'Arcy v Myriad Genetics Inc 2015* (15 December 2015) IP Australia <https://www.ipaustralia.gov.au/sites/g/files/net856/f/examination_practice_following_the_high_court_decision_in_darcy_v_myriad_genetics_inc.pdf>; see also the Australian Patent Office, *Patent Manual of Practice and Procedure, 2.9.2.6: Nucleic Acids and Genetic Information* (11 January 2016) <http://manuals.ipaustralia.gov.au/patents/national/patentable/2.9.2.6_Nucleic_acids_and_genetic_information.htm>.

[31] See Ng, above n 1, 10.

abnormal BRCA 1 gene in a woman's DNA, that information may be indicative of higher susceptibility to breast and ovarian cancer. Medical treatment regimens, clinical care and management therapy can then be structured accordingly. For example, an average woman has a 12-13% risk of developing breast cancer. But women with certain genetic mutations are predisposed to a higher risk of breast or ovarian cancer – e.g. breast cancer risk increases to 50-80% and the risk of ovarian cancer is around 20-50%.[32] The highly publicised case of Angelina Jolie Pitt, a famous American actress and UNHCR global humanitarian ambassador is one example:[33] Jolie Pitt had inherited a mutated BRCA 1 gene that carried an 87% risk of her developing breast cancer and a 50% risk of ovarian cancer.[34] She had lost her mother, grandmother and aunt to cancer. Armed with this knowledge, in 2013, Jolie underwent a preventive double mastectomy. Two years later, she underwent a second preventive surgery to remove her ovaries and fallopian tubes.[35] This case illustrates how the discovery of the BRCA 1 gene mutation can impact on a woman's choice of treatment regimen.

Although the BRCA genes were known to exist in nature, no one had isolated them such that they could be effectively used. Myriad had expended considerable effort and money in isolating the BRCA genes, albeit through the use of well-known and well-established techniques. This feat has generated a storm of global debate on whether the grant of a patent is the most appropriate reward for such research activities.

VI CONCLUSION

The author recognises that there may be merit in a diversity of approaches on how the balance should be struck between private rights and public access, particularly at the intersection of patent law and biotechnology. Yet on certain aspects of patent law, such as those pertaining to human gene patent-eligibility, the benefits of potential convergence may outweigh the costs in promoting a more innovation-friendly and public interest oriented environment.[36] As this is a nascent field, there are serious risks that potentially legitimate innovative activities and patient access may be impeded. The author examines this issue through a comparative study on the approaches adopted in India and US,[37] as well as, Australia – three highly distinct nations that offer "unique contrasts in

---

[32] Data is as reported in the court decisions of *AMP v Myriad*, e.g. USCAFC, US Supreme Court.
[33] The data for this segment is derived from the author's earlier work, see Ng, above n 1.
[34] See Angelina Jolie, 'My Medical Choice', *New York Times* (New York) 14 May 2013, A25.
[35] See Angelina Jolie Pitt, 'Angelina Jolie Pitt: Diary of a Surgery', *New York Times* (New York), 24 March 2015, A23.
[36] See Ng, above n 1.
[37] Ibid.

a comparative analysis of their patent regimes"[38]. Where a concurrence is achieved based on the delineation of clear limits informed by doctrinal and policy considerations among highly divergent nations - it may be that such an approach indeed strikes the better balance between granting private rights without jeopardising public access.

With its landmark decision, Australia has joined the US (and possibly India) in going against the tide of developed countries that uphold the patent-eligibility of isolated DNA. It is perhaps a missed opportunity for this issue to be tested in Canada – the challenge by the Children's Hospital in Eastern Ontario against a global biotechnology company was settled, so the Canadian legal position on gene patents remains at status quo.[39]

Nevertheless, only time will tell whether ultimately this better approach which has been adopted by India, US and Australia will mark the start of a global U-turn in the right direction in respect of human gene patenting.

---

[38] Ibid.

[39] See Richard C Owen, *Dodged bullet or missed opportunity with CHEO settlement?: Richard Owens for the MLI IP newsletter* (12 May 2016) Macdonald-Laurier Institute <http://www.macdonaldlaurier.ca/dodged-bullet-or-missed-opportunity-with-cheo-settlement-richard-owens-for-the-mli-ip-newsletter/>; Noel Courage, *Gene Patents Remain Valid in Canada* (20 March 2016) Bereskin & Parr <http://www.bereskinparr.com/index.cfm?cm=Doc&ce=downloadPDF&primaryKey=735>; Sheryl Ubelacker, *Status of gene patents in Canada unresolved, despite successful challenge* (20 March 2016) CTV News <http://www.ctvnews.ca/health/status-of-gene-patents-in-canada-unresolved-despite-successful-challenge-1.2824957>.

Intellectual Property and Free Trade Agreements: A Call to Return to Basics

Bryan Mercurio*

As a free trader with a slightly libertarian bent, I am excited when barriers to trade tumble and become confused, saddened and even frightened when populists vilify the reduction of trade barriers as being against the interests of the working population.[1] Lower barriers broaden choice and reduce prices on both inputs and finished products. Conversely, barriers that reduce imports restrain markets from performing efficiently and raise costs. For instance, if a country makes imports of steel uncompetitive through tariffs or other barriers it is not just the users of steel who pay for the increased cost, these price hikes are also felt by consumers who pay more for home construction, automobiles and all other products that use steel as an input.

Not being a true devotee of the Austrian School of Economics,[2] I also recognise that in certain instances markets fail.[3] When markets do not perform efficiently there needs to be a lever, pulled by government, which attempts to restore order. Such is the case with intellectual property rights (IPRs), and especially the focus of this essay – patents in pharmaceuticals. Pharmaceuticals take time and an incredible amount of monetary resources to develop and

---

* Professor and Vice Chancellor's Outstanding Fellow of the Faculty of Law, The Chinese University of Hong Kong.

[1] The perfect examples here are US presidential candidates Donald Trump and Hilary Clinton. See Veronique de Rugy, *On Trade, Trump and Clinton Are Indistinguishable and Wrong* (17 August 2016) The National Review (online) <http://www.nationalreview.com/corner/439104/trade-donald-trump-hillary-clinton-bad-policy>; 'Where Hillary Clinton and Donald Trump Stand on Economic Issues', *The Wall Street Journal* (online), 11 August 2016 <http://graphics.wsj.com/elections/2016/donald-trump-hillary-clinton-on-the-economy/>; Heather Long, *Clinton suddenly sounds a lot like Trump on trade* (11 August 2016) CNN.com (online) <http://money.cnn.com/2016/08/11/news/economy/hillary-clinton-trade/>.

[2] Although I respect and see merits in teaching of Carl Menger, Ludwig von Mises, Friedrich Hayek and subsequent disciples, my personal view is that there is a role for the state in creating and setting the conditions for a proper legal environment in which competition and the economy can flourish and yet at the same time be true to the principles of a free market. My present views are perhaps best encompassed by ordoliberal theory, which became known in Germany as (or heavily influenced, depending on perspective) the 'Social Market Economy'.

[3] It should be noted that the Austrian School of Economics is ambiguous on the necessity of IPRs. For an argument at IPRs are not compatible with Austrian economics, see Stephan Kinsella, 'Against Intellectual Property' (2001) 15(2) *The Journal of Libertarian Studies* 1 <https://mises.org/library/against-intellectual-property-2>.

bring to market,[4] yet most are extremely easy and inexpensive to produce. In a free market, it would not make any sense for a company to spend years and between US$1.5-2.6 billion dollars on research and development (R&D) when the finished product could be reproduced and sold onto the market by anyone with the technical capability. Simply stated, there is no incentive to create without even the chance of an economic return.

For this reason, governments intervene and provide for the protection of IPRs. While some form of patent has been granted since at least 1450, both the protection and enforcement have evolved throughout the centuries. Intellectual property rights are territorial in nature, but since 1995 have been directly incorporated into the international trade system through the World Trade Organization's (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).[5] The TRIPS Agreement provides minimum standards on a range of IPRs (including most notably copyright, patents and trademarks) and a somewhat harmonised version of protection and enforcement among the over 160 Members of the WTO. With membership encompassing over 96% of world trade,[6] in essence the WTO and obligations set out in the TRIPS Agreement have become the minimum 'adequate' world standard. In regards to patents, and in accordance with Article 27.1 of TRIPS, patents 'shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application … [P]atents shall be available and patent rights enjoyable without discrimination as to the place of invention, the field of technology and whether products are imported or locally produced'. Substantively, TRIPS prevents third parties not having the owner's consent from the acts of making, using, offering for sale, selling, or importing for these purposes that product (or in the case of process patents, the product obtained directly by that process).[7] The TRIPS Agreement provides that patent

---

[4] The cost of developing a new drug is largely unknown, and always controversial. In 2014, the Tufts Center for the Study of Drug Development estimated the cost of developing a new drug that obtains marketing approval to be $2.558 million. See Tufts Center for the Study of Drug Development, *Cost to Develop and Win Marketing Approval for a New Drug Is $2.6 Billion* (18 November 2014) <http://csdd.tufts.edu/news/complete_story/pr_tufts_csdd_2014_cost_study>. In 2012, the Office of Health Economics (OHE) at the University College London estimated the cost of development to be $1.5 billion. See Jorge Mestre-Ferrandiz, Jon Sussex and Adrian Towse, *The R&D Cost of a New Medicine* (December 2012) Office of Health Economics <https://www.ohe.org/publications/rd-cost-new-medicine>.

[5] *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1867 UNTS 299, ILM 1997 (entered into force 1 January 1995) annex 1C (*Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)*').

[6] World Trade Organization, *Handbook on Accession to the WTO* (August 2007) <https://www.wto.org/english/thewto_e/acc_e/cbt_course_e/intro_e.htm>.

[7] See *TRIPS* art 28.

protection be granted for a minimum period of twenty years from the date of filing.[8]

Since the coming into force of the TRIPS Agreement, so-called 'TRIPS-Plus' provisions have been appearing as part of IP chapters in free trade agreements (FTAs). The aim is to provide for further, deeper and broader protection than that required in the TRIPS Agreement, on all forms of IPRs and including, *inter alia*, the inclusion of additional protectable subject matter, broader and more extensive standards of protection, enhanced enforcement mechanisms and a weakening of 'flexibilities' and 'special and differential treatment' granted to developing and LDCs in the TRIPS Agreement.[9]

Using pharmaceutical patents as an example, this essay argues the maximalist approach to IPRs has gone too far in tilting the balance towards protection and away from public access. It calls for a step back, and argues that trade agreements should only include the core linkage between IPRs and trade – border measures relating to counterfeits and piracy. Section II briefly discusses the extension of IPRs from TRIPS to FTAs and questions the maximalist approach on both a conceptual and practical level. Section III traces the history of IPRs in trade agreements and argues for a more limited place for IPRs in FTAs. Section IV briefly concludes.

I BEYOND TRIPS

Owing to the well-publicised difficulties the WTO has experienced in completing the Doha Round of trade negotiations, FTAs have proliferated at an extraordinary rate since the early 2000s.[10] In regards to patents and pharmaceuticals, TRIPS-Plus provisions have extended protection far beyond what is set out in the TRIPS Agreement. Common provisions appearing in FTAs include requirements to extend patent protection beyond the 20 year period if the patent is not granted within a certain number of years from the date of application, to provide an additional time period of protection for delays in the granting of marketing approval, to protect pharmaceutical test data for a set period of years, restrictions or prohibitions of the granting of marketing approval for generic products when the product at issue is subject

---

[8] Ibid art 33.

[9] Importantly, and unlike Article XXIV of the GATT, Article 4 of the TRIPS Agreement does not exempt FTAs from the MFN principle. Thus, any member that grants 'any advantage, favour, privilege or immunity' to the nationals of *any* other country (whether a WTO Member or not) must accord the same treatment to the nationals of other WTO Members.

[10] See generally, Simon Lester, Bryan Mercurio and Lorand Bartels, *Bilateral and Regional Trade Agreements: Commentary and Analysis* (Cambridge University Press, 2nd ed, 2016).

to patent protection and restrictions on the right to grant a compulsory licence and/or make use of other flexibilities contained in the TRIPS Agreement.[11]

The push for enhanced protection is understandable given that the effective patent term of a pharmaceutical is 8-12 years – patents are applied for prior to the conclusion of clinical trials and must demonstrate safety and efficacy through extensive review from the health department or other relevant government agency prior to being allowed to place the drug on the market. This is unlike almost all other forms of invention, so efforts to ensure an effective monopoly sales period seem reasonable.[12]

I would agree that IPRs have a place in the WTO, as most traded goods embody some form of IPRs and thus IPRs are inextricably linked with trade. Moreover, I understand the politics behind the situation – the industry wanted more than what they received in the TRIPS Agreement and are pursuing other avenues to achieve the desired level of protection. I question, however, the maximalists approach to IPRs being negotiated into FTAs for a number of reasons.

At the conceptual level, the ever-increasing standards being negotiated into FTAs appear to run counter to the goals and objectives of such agreements; that is, freer flowing, more liberalised trade. Patent protection is a barrier to trade; and while it may be viewed as a necessary barrier in order to discourage "unfair" competition and encourage and advance scientific discovery and innovation it is nevertheless the antithesis of "free trade". Likewise, there seems to be something unsettling about resolving public policy issues effecting health and access to medicines in an FTA, as opposed to a more targeted dialogue and forum. There are also major issues with the manner in which TRIPS-Plus provisions are being negotiated into FTAs. Foremost among these is the harmonised approach taken in most negotiations. Far from recognising differences in levels of development, context and regulatory systems, most FTAs negotiated by the major economies seek to instil a uniformed approach that in the main promulgates the domestic system of the *demandeur* onto the partner countries. We see this in all forms of IPRs, from copyright with extended protection periods to the recognition of technological protection mechanisms (TPMs) and their enforcement and certainly in regards to patents.

---

[11] Michael Handler and Bryan Mercurio, 'Intellectual Property' in Simon Lester, Bryan Mercurio and Lorand Bartels (eds), *Bilateral and Regional Trade Agreements: Analysis and Commentary* (Cambridge University Press, 2nd ed, 2016) 324.

[12] In Australia, the Therapeutic Goods Administration (TGA) – part of the Department of Health and Ageing – is the responsible regulatory agency for therapeutic goods, including prescription medicines, vaccines, sunscreens, vitamins and minerals, medical devices, blood and blood products. See Therapeutic Goods Administration, *Home* <https://www.tga.gov.au/>.

Focusing on pharmaceutical patents, we see this in the requirement to extend patent protection periods as a result of 'unreasonable' delays in the granting of a patent (defined by a set period of time) or in the granting of market approval, to the protection of clinical test data to more complex areas of regulation.

This trend is perhaps most notable in so-called 'patent linkage' provisions, which tie the granting of marketing approval by the relevant health agency to patent status. First created in the US in 1984 as part of the Hatch-Waxman Act, patent linkage was part of a 'grand bargain' designed in part to increase the share of generic pharmaceuticals in the market.[13] Prior to this Act, the US treated test data as a trade secret and thus it was unavailable to generic competitors, who would have to re-conduct expensive and time consuming clinical trials in order to enter the market. The Hatch-Waxman Act gave generic competitors access to the test data, but provided safeguards and sweeteners to the industry in the form of, *inter alia*, patent linkage. Subsequent to the Act, the share of generics in the market rose substantially.[14] Perhaps patent linkage was a fair price to pay. But in other markets the context is different, and the arrival of patent linkage has crushed generic competition and delayed its entry into the market. Perhaps nowhere was this more apparent than in Canada, where until the introduction of patent linkage as part of its trade agreement with the US in 1989 and the North American Free Trade Agreement (NAFTA) in 1993 Canada operated a system of compulsory licensing of medicines which facilitated locally manufactured generic medicines.[15] Upon the introduction of patent linkage, it became much more difficult to facilitate generic entry into the marketplace. In this regard, such a harmonised, undifferentiated approach to the negotiation of TRIPS-Plus provisions in FTAs can run counter to health policy; simply stated, what is appropriate for one nation may not be appropriate for others.

---

[13] *The Drug Price Competition and Patent Term Restoration Act of 1984,* 21 USC § 355(b)(1)(A) (1984). For background, see Gerald J Mossinghoff, 'Overview of the Hatch-Waxman Act and its impacts on the Drug Development' (1999) 54 *Food and Drug Law Journal* 187; Robin J Strongin, 'Hatch-Waxman, Generics, and Patents: Balancing Prescription Drug Innovation, Competition, and Affordability' (Background Paper, National Health Policy Forum, 21 June 2002) <www.nhpf.org/library/background-papers/BP_HatchWaxman_6-02.pdf>.

[14] See Henry G Grabowski and John M Vernon, 'Brand Loyalty, Entry, and Price Competition in Pharmaceuticals after the 1984 Drug Act' (1992) 35 *Journal of Law and Economics* 331; Henry G Grabowski and John M Vernon, 'Longer Patents for Increased Generic Competition in the US: The Waxman-Hatch Act after One Decade' (1996) 10 *Pharmacoeconomics* 110.

[15] See Margaret Smith, 'Patent Protection for Pharmaceutical Products' (Background paper No BP-354E, Library of Parliament: Parliamentary Research Branch, Parliament of Canada, 1993); Christopher Scott Harrison, 'Protection of Pharmaceuticals as Foreign Policy: the Canada-U.S. Trade Agreement and Bill C-22 versus the North American Free Trade Agreement and Bill C-91' (2001) 26 *North Carolina Journal of Law & Technology* 457, 507 (fn 282); Milan Chromecek, 'The Amended Canadian Patent Act: General Amendments and Pharmaceutical Patents Compulsory Licensing Provisions' (1987) 11 *Fordham International Law Journal* 504, 527-528.

Moreover, and more than a little concerning, is that the increasingly enhanced protection being negotiated into FTAs is being done without any empirical basis. On the contrary, the evidence clearly demonstrates that increased protection does not always mean increased innovation. There is a point at which increased protection may mean more patents but less innovation; for instance, where cumulative inventions, patent thickets and blocking patents require multiple licenses and it becomes difficult to ascertain what rights exist and to whom they belong.[16] In this context Shapiro states '…stronger patent rights can have the perverse effect of stifling, not encouraging innovation.'[17]

Moreover, evidence exists which also demonstrates that stronger patent protection leads not to enhanced innovation or an improvement in overall welfare, but to firms protecting their interests by advocating even more protection.[18] This seems to be especially the case in pharmaceuticals (but also high-tech products) where firms divert resources away from R&D and into lobbyists and lawsuits in an effort to expand protection. Such behaviour has been labelled the political economy effect, where patent protection keeps increasing due to the lobbying efforts of entrenched firms, and without regard to the system as a whole.[19] In the view of Boldrin and Levine, such behaviour distorts to the optimum range of protection and unbalances the entire system.[20]

In conclusion, given the evidence suggests that 'policy changes that strengthen patent protection … [do] not spur innovation,'[21] it is unsurprising that 'there is widespread unease that the costs of stronger patent protection may exceed the

---

[16] Joseph Stiglitz, 'Economic Foundations of Intellectual Property Rights' (2008) 57 *Duke Law Journal* 1693 ("[a] poorly designed intellectual property regime … can actually impede innovation").

[17] Carl Shapiro, 'Navigating the Patent Thicket: Cross-Licenses, Patent Pools, and Standard Setting' In Adam Jaffe, Josh Lerner and Scott Stern (eds), *Innovation Policy and the Economy* (MIT Press, 2001) 119–50; See also Catherine Tucker, 'Patent Trolls and Technology Diffusion' (Working paper, MIT Center for Digital Business, 2011) <http://ebusiness.mit.edu/research/papers/2011.12_Tucker_Patent%20trolls%20and%20Techonology%20Diffusion_305.pdf>.

[18] William Landes and Richard Posner, *The Economic Structure of Intellectual Property Law* (Harvard University Press, 2003).

[19] Michele Boldrin and David K Levine, 'The Case against Patents' (2013) 27(1) *Journal of Economic Perspectives* 3.

[20] Ibid.

[21] Josh Lerner, '150 Years of Patent Protection' (2002) 92(2) *American Economic Review* 221; *Using Intellectual Property Rights to Stimulate Pharmaceutical Production in Developing Countries: Reference Guide*, UNCTAD/DIAE/PCB/2009/19 (2 May 2011).

benefits'.[22] Despite the unease (and without empirical backing), however, industry efforts to maximise protection have been successful in FTAs.

II TAKING A STEP BACK[23]

The incorporation of IP into the world trading system was not about increased innovation. To the contrary, it is difficult to find any historical evidence in which a negotiating government or corporate interest argued that the proliferation of minimum IP standards would lead to increased innovation. In fact, the term 'innovation' only features once in the agreement, with Article 7 ("'Objectives'") stating:

> The protection and enforcement of intellectual property rights should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.

Other than that, there is an indirect reference to innovation in the fifth recital of the preamble of TRIPS that rather vaguely recognises underlying public policy objectives, including developmental and technological objectives, for the protection of IPRs. If innovation were the driving force behind the TRIPS Agreement one would have expected it to appear more prominently throughout the text; instead, the record is pretty clear that the driving force was the desire of certain developed countries and related private interests to increase minimum standards and enforcement norms in developing countries.[24]

By the late 1970s, most developed nations shifted from a manufacturing or agricultural focus to embrace their comparative advantage as knowledge-based economies. Developing countries, likewise, embraced their advantage in cheap labour and other associated manufacturing costs. Industries in the developed countries – and particularly in the US – began pressing their governments to

---

[22] Adam Jaffe, 'The US Patent System in Transition: Policy Innovation and the Innovation Process' (2000) 29(4-5) *Research Policy* 531.

[23] Much of the information found in this section is also presented in Bryan Mercurio, 'Trade in Pharmaceuticals: Patents and Access to Medicines since TRIPS – Some certainty and several lingering questions' in Julien Chaisse and Tsi-Yu Lin (eds), *International Economic Law and Governance: Essays in Honour of Mitsuo Matsushita* (Oxford University Press, 2016) 427.

[24] See generally Susan K. Sell and Christophe May, *Intellectual Property Rights: A Critical History* (Lynne Rienners Publishers, 2005); Duncan Matthews, *Globalising Intellectual Property Rights: The TRIPs Agreement* (Routledge, 2002).

act and were nearly successful in getting the contracting parties to include a GATT agreement on counterfeiting as part of the Tokyo Round (1973-79) but failed owing to a lack of evidence demonstrating harm to industry, export interests and the overall economy.[25] The issue was again raised at the 1982 GATT Ministerial Meeting[26] and shortly thereafter studies began to be published purporting to demonstrate the amount of harm and loss caused by counterfeiting and piracy of IPRs to industry. The most notable was a 1984 report of the US International Trade Commission, which through survey evidence found that over 70 percent of US production was susceptible to foreign counterfeiting at high cost to the domestic industry:

> [P]roduct counterfeiting is a global business that, according to industry estimates, accounted for $6 billion to $8 billion in lost U.S. and export sales in 1982. Domestic sales lost to counterfeiting and similar trade practices and lost export sales were each estimated at $3 billion and $4 billion.[27]

By 1988, losses to US business were estimated to be 'higher than the loss range of $16-$20 billion'[28] and the US continued to press the case at the GATT. The US efforts were backed up by the then EC, which stated '…the problem of international trade in counterfeit goods has now become of such gravity that urgent action at international level is required.'[29]

---

[25] See *Agreement on Measures to Discourage the Importation of Counterfeit Goods*, GATT Doc. L/4817 (31 July 1979); Matthews, above n 24, 9. See also Susan K Sell, *Private Power, Public Law: The Globalization of Intellectual Property Rights* (Cambridge Studies in International Relations No. 88, 2003) 40-41: 'The push for an IP code in the GATT began in 1978, near the end of the Tokyo Round of negotiations. The Levi Strauss Corporation initiated an effort to combat foreign counterfeiting of its trademark blue jeans. Levi Strauss pressed its case with other trademark-sensitive firms (lobbying as the International Anti-Counterfeiting Coalition) and obtained the backing of the USTR for an anti-counterfeiting code. Owing in part to the eleventh-hour introduction of the proposal, the effort ultimately failed'.

[26] See, eg, *Agreement on Measures to Discourage the Importation of Counterfeit Goods*, GATT Doc. No. L/5382 (18 October 1982). Discussions had continued between industry and governments (notably the US, EC, Canada, Japan and Switzerland) between 1980-82. For more detail on the 1982 Ministerial meeting, see Matthews, above n 24, 9-10.

[27] United States International Trade Commission, *The effects of foreign product counterfeiting on U.S. industry: Final Report on Investigation No.* 332-158 *under Section 332(b) of the Tariff Act 1930* (United States International Trade Commission Publication, 1984) 24.

[28] United States International Trade Commission, *Foreign Protection of Intellectual Property Rights and the Effect on U.S. Industry and Trade Report to the United States Trade Representative, Investigation No. 332-245, under Section 332(g) of the Tariff Act of 1930* (United States International Trade Commission Publication 1988) 4–2.

[29] *International Trade in Counterfeit Goods — Communication by the European Communities*, GATT Doc. No. L/5512 (8 July 1983) 9.

The point of this historical journey is to reiterate what was at the core of the gravitation of IPRs into the multilateral trading system – counterfeits and piracy. Not innovation, not protection within borders and certainly not the search for the optimal effective patent term in regards to pharmaceuticals. Of course, defining 'trade-related' aspects of IP proved difficult,[30] and perhaps was a fool's errand. The negotiations for the TRIPS Agreement controversially expanded in 1989 beyond simply targeting and addressing counterfeits and piracy and became rather larger and all encompassing.[31] While the move provided clarity for negotiators, it was not universally received.[32] In some ways, the TRIPS Agreement became an 'agreement that [recognised] IP is trade-related, in the sense that it recognized that trading partners had a legitimate interest in how, and how effectively, their nationals' IP was protected in one another's jurisdictions'.[33] In this regard, the ever-increasing scope of FTAs into the realm of domestic policy space could be viewed as simply an extension of 'adequate' standards as set out in the TRIPS Agreement. But the argument in this article is that the TRIPS Agreement carefully set out obligations and preserved safeguards,[34] and the encroachment into the preserved domestic space is inappropriate in that it harms domestic needs, circumstances and priorities.

For this reason, the call in this article is to get back to basics and to simply use FTAs as a means to reinforce the TRIPS Agreement in regards to the regulation of border measures. At their simplest, the link is about the IP

---

[30] The record is clear – the negotiating parties did not agree on the meaning of 'trade-related' prior to commencing the negotiations. See *Negotiating Group on Trade-Related Aspects of Intellectual Property Rights, including Trade in Counterfeit Goods*, GATT Doc MTN.GNG/NG11/1 (10 April 1987) (Note by Secretariat) ('Some participants said that they were not clear as to what were the trade-related aspects of intellectual property rights'). The Director of the IP Division of the WTO, Antony Taubman, referred to the negotiating mandate as 'an ambiguous formulation that hovered uncertainly across a range of divergent expectations.' See Antony Taubman, 'Thematic Review' in Jayashree Watal and Antony Taubman (eds), *The Making of the TRIPS Agreement: Personal Insights from the Uruguay Round Negotiations* (WTO, 2015) 38 <https://www.wto.org/english/res_e/publications_e/trips_agree_e.htm>.

[31] See *Uruguay Round – Trade Negotiations Committee – Mid-Term Meeting*, GATT doc MTN/TNC/11 (21 April 1989). For an excellent overview of the mid-term expansion in negotiating mandate, see Antony Taubman, 'The Coming of Age of the TRIPS Agreement: Framing those 'Trade-Related' Aspects' in Christophe Geiger (ed), *The Intellectual Property System in a Time of Change: European and International perspectives* (CEIPI and LexisNexis, 2016).

[32] See Taubman, above n 31, 3 (citing India's concern over the shift). For critical analysis of this expansion in mandate, see Michael Spence, 'Which Intellectual Property Rights are Trade-Related?' in Francesco Francioni (ed), *Environment, Human Rights and International Trade* (Hart Publishing, 2001) 263.

[33] Taubman, above n 31, 4. This includes, in the words of Taubman, 'the idea that there is a category of illegitimate trade that not only may but must be suppressed, inverted basic assumptions about international trade law'; Spence, above n 32, 8.

[34] Taubman shares this view. Taubman, above n 31, 13-14.

embodied in physical goods.[35] It is perfectly reasonable for FTAs to include provisions which expand upon and add more concrete obligations on customs to take certain actions against imports and exports, to enhance procedural issues and provisions on civil and criminal penalties and enforcement more generally and even to require the seizure of infringing goods while in transit.[36] These issues, and countless others, revolve around physical goods crossing the border – that is, being traded. But in other respects, IP Chapters of FTAs have not been about supporting or facilitating freer trade but more so about expanding rights and extracting additional royalties and payments for IP owners. Moreover, the place for setting standards for the grant, administration and/or enforcement of a patent, calibrating an optimal patent term, for delineating he limits of fair use/dealing in copyright and for ensuring geographical indications are adequately prioritised and protected is not an FTA but rather through coherent policy dialogue or through negotiation of an IP-specific agreement.

III CONCLUSION

The negotiation of a comprehensive IP chapter in the NAFTA was perhaps the moment that opened Pandora's Box. Since that time, increasing standards on broader areas of IPRs have been added to subsequent IP Chapters that make almost a mockery of the notion of free trade. Is there 'hope'? Perhaps, but it is only partial hope. The US and other developed country positions are unequivocal and entrenched – but their positions are not the world standard. Multiple mega-regional trade agreements are being negotiated at present in which the parties could take a stand towards the issue and protect only IPRs as they relate to trade, which would reflect the original intent of the incorporation of IPRs into the trade regime. At the very least, this would ensure that the ever-expansive protection of IPRs in FTAs does not eventually find its way into the TRIPS Agreement and become the new multilateral standard. But the

---

[35] Such a link was recognised even before the existence of the TRIPS Agreement. For instance, in 1968 the United Kingdom called Italy's local working requirements for patents and of the manufacturing clause in US copyright law as non-tariff barriers. Boldrin and Levine, above n 19 (citing GATT documents COM.IND/4 (30 August 1968) and COM.IND/4/Corr.1 (26 September 1968)).

[36] The issue of the seizure of goods in transit is controversial, with India and Brazil filing a claim at the WTO against the EU in 2001 over several Dutch seizures of generic medicines. The matter was settled without a panel ever ruling on the case. On the final settlement, see India's Ministry of Commerce and Industry, 'India EU Reach an Understanding on Issue of Seizure of Indian Generic Drugs in Transit' (Press Release, 73554, 28 July 2011) <http://pib.nic.in/newsite/erelease.aspx?relid=73554>. For detailed information and analysis, see Bryan Mercurio, "Seizing' Pharmaceuticals in Transit: Analysing the WTO Dispute that Wasn't' (2012) 61(2) *International and Comparative Law Quarterly* 389.

time for this stand is now, and unfortunately 'hope' may just be contained for some time longer.

Closing Pandora's Box? The EU Proposal on the Regulation of Robots

Burkhard Schafer*

I OF ROBOTS, MYTHOLOGY AND THE LAW

> *Whereas from Mary Shelley's Frankenstein's Monster to the classical myth of Pygmalion, through the story of Prague's Golem to the robot of Karel Capek, who coined the word, people have fantasised about the possibility of building intelligent machines, more often than not androids with human features [...]*

Thus starts the *Motion for a European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics*, submitted by the Committee on Legal Affairs. (henceforth: "the Motion").[1] This paper will attempt a first analysis of key notions of the proposal, by following the proposers in exploring the emerging discourse on robot regulation through the prism of literature and mythology.

The unusual and somewhat tongue-in-cheek introduction is an appropriate reminder of just how much our thinking about robots and their legal regulation is influenced by their depiction in mythology, literature and film. For centuries, we have projected our hopes and fears into human-like machines, seeing in the back-reflection from their metallic (typically) faces an account also of what we are or as what we see ourselves. Law and legal regulation plays a consistent theme in these stories, as we will see below.

II CLOSING PANDORA'S BOX

A reference missing from the Motion is that to the story of Pandora. When juxtaposed to the Genesis account of Eve and the Fall, we get a first idea of the concerns that the committee tries to address. Pandora was created by Hephaestus, blacksmith to the gods and master-engineer. She was designed with one purpose in mind – punishing mankind for acquiring the fire from the

---

* Professor, School of Law, University of Edinburgh.

[1] *Motion for a European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics* [2016] 2015/2103(INL) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN> ('*Civil Law Rules on Robotics Motion*').

gods. Built to allure and to seduce, her task is to deliver the jar that contains all the evils in the world, "burdensome toil and sickness that brings death to men". Only hope remains in the jar before she closes it again.

The story told by Herodotus bears some striking resemblances, but also a crucial difference to that of the Biblical Eve. Eve too is designed – though maybe better described as bioengineered. She too will bring through her actions toil, sickness and disease into the world. But unlike Pandora, who acted strictly according to her instructions, with Eve it is the ability for autonomous decision making and with that the ability to act in ways unforeseeable to her creator that causes the harm.

Today we find the same topoi in the highly gendered depiction of robots in film - Ava, the robot in Ex Machina, just like Pandora is designed to seduce, just like Eve ultimately through her autonomy bringing doom on the naïve man she interacts with. Maybe even more worrying, real life examples of robotics follow the same patterns, with the female Siri and Tay playing the role of secretary, while the male chatbot Ross[2] delivers proper legal advice.

Exploring how gender and fear shape our perception of robots would go beyond the scope of this paper.[3] But Pandora and Eve, each in their own way, encapsulate the fears and concerns that dominate the legal debate on robotics: One is the concern that malicious designers could develop deadly robots intentionally to inflict harm on humans. Concerns that have led to calls to outlaw military application of robotics. The other is the fear that by creating entities with autonomy and permitting them to act in ways that may be in principle unpredictable by us, we are not only engaging in risky behavior, we might sever the nexus between creator and creation that allows us to attribute legal liability and responsibility if things go wrong. Just as Eve's action plays a central role in Christian apologetics, so robot autonomy is seen as a potential "get out of jail card" that could be played by manufacturers or sellers if their products cause harm.

Or, in the words of the committee on the reasons for taking action at sec. 24: "whereas, notwithstanding the scope of the Directive 85/374/EEC, the current legal framework would not be sufficient to cover the damage caused by the new generation of robots, insofar as they can be equipped with adaptive and learning abilities entailing a certain degree of unpredictability in their

---

[2] Karen Turner, 'Meet 'Ross,' the newly hired legal robot', *Washington Post* (online), May 2016 <https://www.washingtonpost.com/news/innovations/wp/2016/05/16/meet-ross-the-newly-hired-legal-robot/>.

[3] See, eg, Friederike Eyssel and Frank Hegel,'(S)he's Got the Look: Gender Stereotyping of Robots' (2012) 42(9) *Journal of Applied Social Psychology* 2213.

behaviour, since these robots would autonomously learn from their own, variable experience and interact with their environment in a unique and unforeseeable manner."[4]

The fear is that this could expose buyers and the general public to harm without recourse. It could equally however create uncertainty for manufacturers, sellers and investors that prevents the robotics industry realising its beneficial potential. Law, appropriately adjusted to this new reality, might be able to give us reasonable hope in a safe robotic future. Yet hope, as Pandora's story shows, is an ambivalent concept. It is unclear if by keeping hope in the jar, Pandora denied us "even hope" and punished us even more, or if closing the lid was an act of kindness – after all, hope was placed by Zeus in a jar that contained all evils, and what is more evil than hope continuously disappointed. Is the Motion then aimed to "close the box" in the sense of keeping a lid on potential harm? Or is it giving us "false hope", in that it deludes us into thinking that by regulating a technology we can make it safe?
Or is the role of the proposal merely symbolic, a form of "red flag" law that does not address any real problem, but responds to public concerns by creating unnecessary and to a degree burdensome duties on robotics manufacturers, but with the advantage of increasing public acceptance of the technology? These are some of the themes that this paper will explore.

III THE LAW AND THE GOLEM

The EU Motion prominently mentions the story of the Golem as one of the oldest examples of man-made autonomous machines. If the Golem was the first robot, then a lawyer was the first roboticist. Tractate Sanhedrin 65b from the Talmud (the "cases and materials" of Jewish law) describe how amora (legal scholar) Rava created in the 3rd century BCE a person-like being from mud. Rava was one of the most influential law teachers of his time, contributing to the canon of Talmudic law a concept of good faith acquisition of lost/abandoned property; and to the laws of civil procedure a secularised notion of witness credibility assessment. That it should be a lawyer who created the first robot is within the Jewish religious framework entirely understandable: God is (perfect) law and the ultimate creator, so everyone who achieves near-mastery of the law could arguably also achieve near-mastery of the art of creation. Near-mastery only though, and indeed Rava's robot quickly failed the Turing test: When Rava, maybe to put his work to the test, sends him on an errand to another influential amora, Rav Zeira, the man-machine is quickly found out. Incapable of answering questions directed at it, Zeira easily identifies the originator behind the ploy: "You were created by the sages;

[4] *Civil Law Rules on Robotics Motion*, 6.

return to your dust".[5] Then and now, the ability to display human characteristics when under cross-examination and responding appropriately to questions was the litmus test that distinguishes man from machine; then and now, mastering language turns out to be a difficult task to achieve.

The idea of lawyers as arch-roboticists quickly disappears from history, though it returns briefly in the 19th century with an interesting twist. Legal formalism developed an ideal of the judge as adjudicator that saw them as machine-like in nature, working through simple algorithms, ideally available in codified form, to determine the right outcome without fear, favor, or any other emotion for that matter. Roscoe Pound dismissively termed this "mechanical jurisprudence",[6] but for some of its adherents this epithet would have been a source of pride rather than disparagement. Over 100 years before Pound, Julian de la Mettrie wrote in "Machine Man":

> To be a machine and to feel, to think and to be able to distinguish right from wrong, like blue from yellow [...].[7]

Rather than making robots like their Jewish predecessors, the legal formalists of 18th Europe dreamt of turning themselves into machines. From this two themes emerged that are also relevant for the contemporary discussion on robot regulation.

The first is the idea, central for formalist jurisprudence, that legal codes can be seen as a library of rules, which together with an appropriate logic form an algorithm that can determine mechanically the outcome of a case. This idea, which informed the development of first generation legal expert systems such as Taxman[8] or the Latent Damage System,[9] also opened up the possibility of a different approach to robot regulation. Rather than using law only retrospectively, after a violation has occurred, implementing formal representations of relevant legislation in the robot's software might ensure law compliance by design. This idea was popularized in literature through Asimov's famous Laws of Robotics – though we should note that their main narrative function is to create problems and to require workarounds. Asimov

---

[5] David Honigsberg, 'Rava's Golem' (1995) 7 *Journal of the Fantastic in the Arts* 137.
[6] Roscoe Pound, 'Mechanical Jurisprudence' (1908) 8 *Columbia Law Review* 605.
[7] Julien Offray de La Mettrie, *Man Machine and Other Writings* (Cambridge University Press, 1996) 35.
[8] Thorne McCarty, 'Reflections on Taxman: An Experiment in Artificial Intelligence and Legal Reasoning' (1997) 90 *Harvard Law Review* 837.
[9] Richard Susskind 'The latent damage system: a jurisprudential analysis' (Paper presented at Proceedings of the 2nd international conference on artificial intelligence and law (ICAIL 89), University of British Columbia, Vancouver, 1989) 23–32.

did not advocate them as a solution, if anything, his stories show how difficult it can be to reduce normative decision making to simple rule following. However, the idea got traction in the legal domain. The first commercially deployed example was through DRM as a form of copyright law by design, and more recently through the "privacy by design" requirement, encouraged by implication in the EU Data Protection Directive, and soon to be explicitly mandated in Art 25 of the EU General Data Protection regulation.[10] Lessig's influential (and highly critical) appraisal of software-enforced rule compliance finally brought the equivalence between legal and software code into the mainstream discussion on technology regulation.

The Motion to the EU Commission remains deeply ambivalent on this issue. Citing explicitly Asimov, it states as General Principle L that:

> whereas, until such time, if ever, that robots become or are made self-aware, Asimov's Laws must be regarded as being directed at the designers, producers and operators of robots, since those laws cannot be converted into machine code;[11]

It is unclear why the committee thinks that self-awareness is a precondition for legal rule following. It is true that the rules in the form given to them by Asimov are too general and abstract to be suitable candidates for a formal capture that could guide machine behaviour. However this does not mean that quite sophisticated formal representations of legal norms can't under the right conditions be an effective tool for robot regulation. The committee seems to recognise this when at sec 10, it also:

> calls, in this regard, on the Commission to foster the development of standards for the concepts of *privacy by design* and privacy by default, informed consent and encryption;

It seems clear that despite the dismissive reference to Asimov's laws in the general part, some form of legal reasoning capacity will have to play a role in the tool set for efficient robot regulation. Given just how prevalent robotic devices are bound to become, we will therefore likely face a future of "ambient law", where gadgets, cars, automated homes or smart cities constantly run algorithms that are isomorphic formal representations of relevant legal provisions.

---

[10] *Regulation (EU) 2016/… of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119.

[11] *Civil Law Rules on Robotics Motion*, L .

The second lesson that we can learn from the 19th century idea of turning lawyers into robots concerns the effect of robotics on the labour market. We find the idea that modern working practices are turning humans into machines prominently in Karel Čapek's play R.U.R. from 1920, which the EU Motion also cites. The heroine of the book, Helena, is a representative of the "League of Humanity", a human rights organisation that lobbies for employment and other civil rights for robots, including the right to get paid fair wages. The impact of these robots on the labour market and wider society is however as profound as it is ambivalent, resulting in deskilled humans with decreasing birth rates and ultimately little to protect them when the robot uprising begins. While for Čapek, robots were a metaphor for dehumanising working conditions under modern modes of production, the fear that robots will disrupt our labour markets and put additional strain on already overstretched social security systems also plays a central role in the current debate.[12] It is also a concern in the EU proposal that states at Para 20:

> Bearing in mind the effects that the development and deployment of robotics and AI might have on employment and, consequently, on the viability of the social security systems of the Member States, consideration should be given to the possible need to introduce corporate reporting requirements on the extent and proportion of the contribution of robotics and AI to the economic results of a company for the purpose of taxation and social security contributions; takes the view that in the light of the possible effects on the labour market of robotics and AI a general basic income should be seriously considered, and invites all Member States to do so.[13]

With this the Motion opens up for discussion two of the more radical proposals for a wider societal response to increased automation at the workplace. One is to abandon the notion of employment as the norm, and of wages as the typical form of income. Instead, a general basic income is suggested as an alternative should, as some commentators have predicted, the reduction in available jobs overwhelm existing social security networks.[14] A possible source for funding of such a scheme is also hinted at by the EU committee. Robots could be treated as employees for tax and social security purposes. While not exactly getting paid, as Helena lobbied for in R.U.R,

---

[12] See,eg, Martin Ford, *Rise of the Robots: Technology and the Threat of a Jobless Future* (Basic Books, 2015).

[13] *Civil Law Rules on Robotics Motion*, 23.

[14] On basic income and robot technology see in particular, James Hughes, 'A strategic opening for a basic income guarantee in the global crisis being created by AI, Robots, desktop manufacturing and BioMedicine' (2014) 1 *Journal of Evolution and Technology* 45.

robots could be paying income tax – or rather a levy could be raised from companies that splits the difference between the reduction of costs that the company gains through automation and the costs that this creates for the welfare system through loss in tax revenue and increased demand for unemployment benefits.

This suggestion raises an interesting philosophical question with direct legal relevance: How do we count robots, and how do we identify individual specimens? If a company owns one hundred cars, each with identical software, all communicating constantly with each other and a central server, is this one (distributed) robot, or one hundred? If the latter, why would an autonomous car, which will have several hardware and software components that constantly talk to each other and a central processor, not also count as several robots? Furthermore, as the software of a robot will in most cases require constant updating, since software ages faster than hardware. But is a robot that undergoes a radical change in its software still the same – or should it be considered as a new employee?

Čapek's story also brought to the fore the possibility that robots should be recognised as legal persons, and with that another important crossover between law, literature and robotics. Using the law to resolve conflicts caused by the autonomy and intelligence of machines is a recurrent theme in 20th century robot literature. It is through a legal trial that Commander Data in the Startrek universe has to prove that he is deserving of legal protection and the status of a legal person. Formal confirmation of citizenship and the rights and duties that it entails to the robot Johnny Five brings the "Short Circuit" franchise to a conclusion. These and similar stories evidence how much we still trust the law as a vehicle to settle social and political disputes. In a case of life imitating art, the mayor of Nanto City granted in 2010 the therapeutic seal robot Paro a "koseki" (household registry/birth certificate), which lists Shibata Takanori, Paro's inventor, as the robot's father.[15]

The idea of robots as holders of rights has been mooted on and off in the academic discussion for quite some time, but never attracting significant support.[16] A Horizon scanning report for the UK government however took the idea serious enough to contemplate limited civil rights for robots within

---

[15] For a discussion see Jennifer Robertson, 'Human rights vs. robot rights: Forecasts from Japan' (2014) 46 *Critical Asian Studies* 571.

[16] See, eg, Hilary Putman, 'Robots: Machines or Artificially Created Life?' (1964) 61 *The Journal of Philosophy* 668; David J Gunkel, 'A vindication of the rights of machines' (2014) 27 *Philosophy & Technology* 113; Mark Coeckelbergh, 'Robot rights? Towards a social-relational justification of moral consideration' (2010) 12 *Ethics and Information Technology* 209.

the next 50 years.[17] At first sight the EU Motion appears to follow this line of thought and asks to at least contemplate the possibility of:

> creating a specific legal status for robots, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons with specific rights and obligations, including that of making good any damage they may cause, and applying electronic personality to cases where robots make smart autonomous decisions or otherwise interact with third parties independently.[18]

Together with the notion of robots as tax payers, this idea led commentators in the popular press to the conclusion that the EU is indeed preparing the ground for legal recognition of robots, possibly in analogy to the legal status of corporations. A more cautious reading of the proposal however would replace "right" in the above section with "capacity", in particular the capacity to enter into legal agreements that are binding on the owner. As a simple example, we can think of an automated car that pays any applicable road tax "on its owner's behalf".

If read like this, we can see that the discussion is far from new. At the turn of the century, advances in the design of autonomous agent software led to concerns about the legal status of contracts that were negotiated between machines, with no or limited human oversight. The "law of electronic agents" workshop series that was held as part of the EU funded Agentlink network addressed these issues comprehensively. The emerging consensus at the time indicated that radical solutions such as ascribing legal personality to software agents was unnecessary, and that existing legal instruments were capable of dealing with machine-to-machine contract negotiations in an equitable way.[19]

IV ROBOTS OR AI

Why would the committee feel the need to reopen this discussion? Part of the reason is the very definition of "robot" that the Motion suggests, and to which we will turn our attention now.

---

[17] *Robots could demand legal rights* (21 December 2006) BBC News <http://news.bbc.co.uk/1/hi/technology/6200005.stm>.

[18] *Civil Law Rules on Robotics Motion*, 31F.

[19] See, eg, Emily Weitzenboeck, 'Electronic agents and the formation of contracts' (2001) 9 *International Journal of Law Information Technology* 204; Giovanni Sartor, 'Cognitive automata and the law: electronic contracting and the intentionality of software agents' (2009) 17 *Artificial intelligence and law* 253.

The Motion asks the Commission to:

> propose a common European definition of smart autonomous robots and their subcategories by taking into consideration the following characteristics of a smart robot:
>
> - acquires autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and trades and analyses data
> - is self-learning (optional criterion)
> - has a physical support
> - adapts its behaviours and actions to its environment

If adopted, the EU would be the first jurisdiction with a generic definition of robot, to be applied across legal domains. While a small number of jurisdictions has defined the term "robot" in law for specific purposes, they typically are to be found in highly technical laws that deal with issues such as their treatment for tariff purposes (Russia, which uses a rather long and cumbersome definition), facilitate and encourage investment in robotic technology or set aside physical spaces where they can be safely tested. None of these definitions play a direct role in core civil law, or are intended to regulate liability of/for robotic devices. The EU proposal also comes close to definitions used by roboticists. Mataric for instance defines robots as "an autonomous system which exists in the physical world, can sense its environment, and can act on it to achieve some goals."[20]

While the proposed definition is in line with that used within the technology community, reasonably flexible to anticipate future developments and sufficiently precise, it is nonetheless questionable if it is adequate for legal purposes. It is premised on the idea that there are certain legally problematic aspects of robots that apply across all or most applications. But are there really legal questions that military robots, care robots for the elderly, medical robots, automated cars, toy robots and advanced washing machines share? The main concern of the committee is clarifying civil liability, but even for such a limited objective, it seems obvious that very different rules apply to different types of robots, or indeed to the same type of robot used in different scenarios and by different actors. Some, but not all robots will simply be consumer goods, and significant parts of their liability hence regulated by consumer protection law. Others will be used by law enforcement and military, including dual–use robots, where the liability regime in many countries cerates special liability rules and exemptions. Medical devices and cars traditionally have their own

[20] Maja J Matari,*The robotics primer* (MIT Press, 2007) 4.

regulatory regimes that already implement some of the suggestions that the committee proposes.

Two key components of the committee's recommendations are a mandatory insurance scheme. Manufacturers or owners insure the robots against harm to the buyer and to third parties. In addition, a supplementary fund is suggested to cover those machines for which no insurance was taken out.[21] In what is possibly the most innovative suggestion in the proposal, monies paid to robots as part of their work could directly flow into this fund, and cover it automatically in case it causes actionable damages. This idea of legally protected funds that "follow the robot" seems to be inspired by the Roman law of slavery.[22] The *peculium* in Roman times was a fund slaves (or indeed sons) could be given to manage for themselves. While ultimately, they were still part of the property of the paterfamilias, in practice, they functioned like property of the slave and could be used to buy his freedom. The committee is not suggesting this use of the peculium, nor do they seem to envisage a peculium that contains again other robots (the way the Roman peculium could). Instead, we could imagine maybe an entry into a blockchain ledger, which then would allow claimants with little bureaucratic efforts or cost to claim "directly" against the robot, without having to determine if the fault was due to software or hardware, the liability the seller's or manufacturer's.

The second component is a mandatory registration scheme, for all robots, for the purpose of

> ...ensuring that the link between a robot and its fund would be made visible by an individual registration number appearing in a specific EU register, which would allow anyone interacting with the robot to be informed about the nature of the fund, the limits of its liability in case of damage to property, the names and the functions of the contributors and all other relevant details[23]

This too could be facilitated through blockchain ledger technology. The problem with this proposal, and one that the committee tacitly admits when it asks the Commission to develop an appropriate classification scheme to determine which machines should be subject to such an approach, is that for those robots that will pose the greatest risks – medical robots and cars – registration and insurance systems already exist. On the other hand, a

---

[21] Committee Motion 31 a and b.
[22] See, eg, Ugo Pagallo, 'Killers, fridges, and slaves: a legal journey in robotics' (2011) 26 *AI & society* 347.
[23] *Civil Law Rules on Robotics Motion*, 31E.

requirement to register and insure every individual Romba, washing machine or robotic toy dog seems vastly excessive.

While the suggested general definition is therefore overly inclusive, and in need to be broken up again by the suggested classification scheme, it is in another respect overly exclusive. "Unembodied AIs", intelligent software agents, are not covered by the definition. Siri or Tay the Apple and Microsoft chatbots, are (probably, but see below) not covered by the definition. This is problematic not only because AIs like these will play such a significant role in changing the way we interact with Information Technology. It also ignores that some of the most pressing legal issues that the Motion tries to address are not only the same for disembodied AI, but have been analysed, discussed and in some cases actioned on successfully in this field. As we saw, this is particularly the case for the question of legal personhood. This issue arises always when an entity, be it machine or software code, is not only to a degree autonomous, but also has the ability to communicate. By excluding unembodied AI, the committee forgoes the chance to learn from the experience legal systems have made with regulating software agents. The most important of these is maybe that the status of the entity itself is less relevant for the discussion. What matters is the status of the speech acts they perform. Once we have decided we want to "count as" contractual offers machine generated speech, the issue of the status of the machine becomes almost irrelevant and we have the choice to treat it as a mere message, as an exercise of the law of agency or indeed "directly" to a legal person. Similarly, if a machine utters the words "I hereby declare you man and wife", it will be a question for administrative or canon law to decide if this can count as a valid performance of a wedding. No general definition of what a robot is in law can or should pre-empt this discussion, to which different legal systems and traditions may well give different answers.

Excluding disembodied AI from the remit of the discussion not only prevents the committee to learn from experience made with these devices, it also prevents a discussion of aspects of the law that may be in much more need of revision than contractual or even core delictual liability.

When Tay, the Microsoft chatbot, was released on Twitter, it quickly picked up (or rather, was forced to pick up through a concerted effort by some users) particularly loathsome ideas and habits. This also means that some of its Tweets could be speech acts of a different legally relevant kind: defamation or criminal insult, or in jurisdictions with relevant legislation criminal hate speech or Holocaust denial. Nobody suggested suing Microsoft though – too obvious was the fact that "Tay was still learning". In the UK, defamation is a strict liability tort however, and to bring the legal ideal in line with the practical reality of learning machines, one might consider carving out a "court jester"

exemption to robot speech in those cases at least when it is clear that the utterance was a result of imperfect learning.

Whenever a robot produces speech, this also creates questions for copyright law. The EU Motion mentions IP but briefly and concludes that in all likelihood, robotics technology is not creating significantly new problems. This is a surprising omission, also given the importance of IP to stimulating technological investment. Some robots produce works of art, for instance Taida, winner of the 2016 Robotart competition.[24] So far, only the UK, and soon Japan, provide for explicit rules on the status of creative works generated by autonomous machines, and whether or not their approach is helping or hindering the evolution of the field needs discussion. Even more important than works of art, the overwhelming amount of data is generated automatically, by autonomous devices and through machine-to-machine communication. Some of this data has commercial value. If my driving trains the AI in my automated car, and the manufacturer can get access to this data to improve their products, do I have a proprietary interest in this data if it is not personal information and protected by data protection law? The commission Motion focuses on questions of liability, but even here IP law matters. For robots will not just be producers, they will also be "consumers" of IP protected work. They are reliant on input from their environment to navigate, learn and improve. Some of this information will in turn be IP protected. Can a drone take images of famous buildings for navigation purposes and share copies with its fleet, potentially violating the IP rights of the architect? Can they data-mine my tweets to improve their speech?

With these observations, our discussion turns full circle. The first robot, the Golem, lacked capacity to communicate. This also meant that many legal issues were pre-empted. The Motion for an EU initiative on robot regulation is an important step to open up the discussion on appropriate, harmonised responses to the robot revolution. Many of its ideas are bold and worthy of discussion, even if few are likely to make it into law. Yet at some crucial points, a major reassessment is necessary. Neither the proposed definition of robot, nor the subsequent focus on liability, seem to have identified some of the most intricate problems or the most pressing legal needs. To start a discussion on legal regulation of robotics with references to robots in literature and mythology was an unusual step to take. It has significant pedagogical advantages, as it reminds us of the fears and hopes that mankind projects into its machines, fears and hopes that then put pressure on legislators to act. Yet, more might have been learned by taking these stories more seriously, with their

---

[24] *TAIDA* (2016) RobotArt <http://robotart.org/archives/2016/team/taida/>.

focus on man-machine cooperation and with that robotic speech. Of greater concern maybe is however that they also create in our mind a vision of robot that for the foreseeable future will be the exception rather than the norm: anthropomorphic, with high degrees of autonomy, multi-purpose and competing rather than cooperating with humans. For this type of robot, the committee proposal makes bold and innovative suggestions worth of further exploration by the EU Commission. But we should be concerned that by extending this regulatory approach across the whole range of robots, we could impede needlessly innovation and investment in some fields, or conversely, this over-extension of the proposal could undermine its merit in those fields where more radical legislative action is beneficial end needed.

An Interview with Professor Brad Sherman*

PB: Brad Sherman, thank you for joining us. To start off with I'd like to ask you about the project you've been working on: *Harnessing Intellectual Property to Build Food Security*. The goal of the project is to minimise the cost and maximise the benefit of using intellectual property to improve agricultural productivity and food security in Australia and the Asia Pacific. What have you found to be the greatest barriers to achieving this goal?

BS: Most of the research to date has been very narrowly focused both in terms of the areas it looks at and the approaches taken. What we're trying to do with the project is to extend our exploration into all aspects of the food chain: the collection of genetic resources, breeding, scientific research, on farm practice, processing, packaging, storage, consumption and waste. At every point along the food chain we're thinking of the potential intellectual property ramifications.

The second thing that we're trying to do is to take what many people have as their conclusions as our starting point. There have been a lot of solutions that have been suggested in the past decade, for example there have been suggestions for defensive patenting of agricultural products through particular libraries or particular clauses in contracts of public or private partnerships. We're going to look at those conclusions as our starting point and critically examine them from an ethnographic, anthropological, historical and critical revisionist perspective. The challenge is to not fall into the same old patterns but to push the debate forward.

PB: Is your work primarily in the Asia Pacific or is it primarily in Australia?

BS: We're looking at Australia, the Asia Pacific and in some cases beyond the Asia Pacific, because food is a global thing. There have been experiments in different countries; we're looking at some of those experiments. The primary focal point for the end product of the project is Australia and the Asia Pacific; however, I have a student in Ecuador at the moment looking at the attempts of the Ecuadorian government to develop new innovative ways to protect food security.

---

* Professor, TC Beirne School of Law, the University of Queensland. This interview was conducted by Madeleine Gifford at the University of Queensland on 3 August 2016.

We're looking at that experiment and drawing lessons that may apply when thinking about the Asia Pacific and Australia.

PB: When dealing with products designed to treat malnutrition, the use of patents can generate criticism. In 2009 Médecins Sans Frontières penned an open letter criticising Nutriset for aggressive enforcement of its patent for Plumpy'nut (a peanut-based paste used to treat severe malnutrition).[1] Despite exempting companies and NGOs in some African countries from paying a licensing fee,[2] Nutriset has been repeatedly criticised and has faced legal action over its Plumpy'nut patent in other regions.[3] In comparison a non-profit humanitarian patent pool in the form of a single licensing authority exists for Golden Rice.[4] The six key patent holders of Golden Rice reached an agreement to allow Potrykus to grant licenses free of charge.[5] A Humanitarian Board was then established to distribute licenses.[6] On face value the patenting system used for Golden Rice seems like a better solution for combating malnutrition, however do you think the strict enforcement of patents pushes innovation and therefore provides a better long-term model?

BS: When people think about patents and intellectual property they often think about it very narrowly. One of the things we're doing is using historical work to broaden the way we think about what patents are and how they work. One of the lessons we're drawing upon is the idea that intellectual property can perform different functions; it doesn't just have to be about protecting investment innovation. In some circumstances it is possible, say in public and private organisations or developing and non-developing countries, to work together to

---

[1] Hugh Schofield, *Legal fight over Plumpy'nut, the hunger wonder-product* (8 April 2010) BBC News (online) <http://news.bbc.co.uk/2/hi/europe/8610427.stm>; Tido von Schoen-Angerer, *MSF: Nutriset patent impeding access to treatment of Severe Acute Malnutrition* (13 November 2009) Médecins Sans Frontières International <http://www.msfaccess.org/content/msf-nutriset-patent-impeding-access-treatment-severe-acute-malnutrition>.

[2] Nutriset, *Nutriset/IRD's Patents Usage Agreement* <http://www.nutriset.fr/en/access/patents-for-development/online-patent-usage-agreement/>.

[3] Umar R Bakhsh, 'The Plumpy'Nut Predicament: Is Compulsory Licensing a Solution?' (2012) 11 *Chicago-Kent Journal of Intellectual Property* 238 <http://scholarship.kentlaw.iit.edu/cgi/view content.cgi?article=1116&context=ckjip>.

[4] Birgit Verbeure, 'Patent pooling for gene-based diagnostic testing: conceptual framework' in Geertrui van Overwalle (ed), *Gene Patents and Collaborative Licensing Models: Patent Pools, Clearinghouses, Open Source Models and Liability Regimes* (Cambridge University Press, 2009) 3, 17.

[5] Ibid.

[6] Pamela Ronald, 'Nutritional enhancement by biofortification of staple crops' in David Bennett and Richard Jennings (eds), *Successful Agricultural Innovation in Emerging Economies: New Genetic Technologies for Global Food Production* (Cambridge University Press, 2013) 199, 213.

simultaneously protect investment and at the same time have humanitarian goals in mind. We're looking at some case studies that involve public sector agencies that have the primary goal of poverty reduction and food security. In certain situations, they have decided to partner with private sector organisations because on their own they don't have the capacity to get their technology to the people they want to get it to. For example, a group in Kenya had developed a mechanism to identify a particular fly-borne disease that was having a dramatic impact upon milk production across West Africa. They identified it but they didn't have the technology or expertise to develop a diagnostic test kit, so they partnered with Syngenta and arranged a specialised contractual arrangement where Syngenta could use the technology exclusively in Australia, Canada, the United States and Europe, but in every other country it had to be freely available. So one of the things we're looking at is how effective those types of revisions are going forward.

PB: It's difficult to talk about patents without also talking about bilateral and multilateral co-operation and trade agreements. The Trans-Pacific Trade Agreement has generated a lot of discussion in regards to its implications for intellectual property law, especially copyright law.[7] In regards to patent law however Australia will not need to do much to meet its obligations and may benefit from the harmonisation of laws, particularly in relation to the 12 month grace period.[8] Do you have any concerns about the TPP or any other agreements?

BS: We are very much focused on the bilateral and multilateral agreements, so it's not really a concern but it's something we're taking into account. One of the things we are doing at the outset is looking at international treaties under which countries have the capacity to and are obliged under TRIPS to pass laws that provide protections for patents, plant genetic resources and plant breeder's rights. We are trying to expand those protections as broadly as possible, using historical work in particular, to say seed certification laws or seed consumption laws are able to fall in the ambit of certain provisions. A developing country is then able to use this to say they have complied

---

[7] Gareth Hutchens, 'ACCC airs concerns over intellectual property provisions in Trans-Pacific Partnership', *The Sydney Morning Herald* (Sydney), 1 December 2015 <http://www.smh.com.au/federal-politics/political-news/accc-airs-concerns-over-intellectual-property-provisions-in-transpacific-partnership-20151201-glcef0.html>.

[8] Department of Foreign Affairs and Trade, *Chapter Summary: Intellectual Property* (12 November 2015) <http://dfat.gov.au/trade/agreements/tpp/summaries/Documents/intellectual-property.PDF>.

with TRIPS and the relevant provisions. The concern I have is that bilateral agreements may not adopt the language of TRIPS, but adopt a much more specific approach, for example, you may have to adopt Australian patent law, and if that happens it becomes phenomenally problematic.

PB: In your book *Figures of Invention*, you track the history of modern patent law.[9] Taking into consideration past events, do you think we're entering into an era of particularly intense patent wars, especially in regards to the smart phone industry,[10] or are intense patent wars a reoccurring trend throughout history?

BS: This is a very common practice and there have been lots of examples. At the beginning of the twentieth century the aviation industry went through the same process, so did the dye and chemical industry. At different periods of time there will be large organisations that fight. It really depends on the makeup of the industry. For example, in the software industry eight or ten large hardware manufacturers compete against thousands of smaller software companies. With the smart phone industry you have two large corporations and intellectual property is just part of the commercial strategy. They'll use it for a while and then use it as a lever to negotiate down the track. It's same old, same old.

PB: On the other hand, some companies have recently allowed potential rivals to use their patented technology. Tesla has promised not to initiate patent lawsuits against anyone who, in good faith, wants to use their technology.[11] For Tesla, developments in new markets could create a shift away from gasoline-powered vehicles towards electric cars. This strategy has also seen a wider application. Facebook has shared once-proprietary information on hardware designs, allowing dozens of companies to build different models, allowing Facebook to simply contract with the most efficient prototype-maker.[12] Is this trend also not a new occurrence?

---

[9] Alain Pottage and Brad Sherman, *Figures of Invention: A History of Modern Patent Law* (Oxford University Press, 2010).

[10] Jessie Lang, 'The Use and Abuse of Patents in the Smartphone Wars: A Need for Change' (2014) 5 *Case Western Reserve University Journal of Law, Technology & the Internet* 239.

[11] Kirsten Korosec, 'Why This Electric Bus Startup Is Opening Up Its Patents for Free', *Fortune* (online), 28 June 2016 <http://fortune.com/2016/06/28/proterra-open-patents/>.

[12] Quentin Hardy, 'Why Tesla gave away all its patents', *Australian Financial Review* (online), 30 March 2015 <http://www.afr.com/it-pro/why-tesla-gave-away-all-its-patents-20150330-1mb0yb>.

BS: There are lots of examples in the past where organisations took out patent protection and then relinquished it. I don't know enough about the details of your example but what I'd be concerned about is the difference between allowing third parties to access technology that's protected and then giving up the patent. It still is potentially protected or protectable, and it would depend on the terms and the conditions of the license that were given to people. Organisations often make a strategic decision because they want people to adopt the technology. If technology becomes standardised, then it's the best business model for them. Patents may provide them with some sort of way to protect it. I don't know enough about the terms and conditions by which the proprietary information or objects are being given out, but it's not unusual.

The Fate of 'Privacy' in an Automated Society

Megan Richardson*

I am grateful to the editors of *Pandora's Box* for suggesting I contribute a short piece for the journal. The article below is based on presentations I gave at a conference on *Defining the Sensor Society*[1] organised by Mark Andrejevic and Mark Burdon at the University of Queensland, and a *Smart Cities* forum hosted by the Victorian Privacy and Data Protection Commissioner David Watts as part of Privacy Week in April 2016.[2] My thinking has evolved a little since these events and the paper has been expanded accordingly.[3]

I FRAMING THE PROBLEM

We live in a society increasingly saturated with smart phones, watches, cameras, fitness monitors, and other intelligent devices combined with interactive social networks and other digital platforms. If one result of all this activity is a transformation in the processes of personal data collection, storage and analysis, another is the pervasiveness and inescapability of the monitoring by these devices and networks.[4] In short, we are witnessing a shift to a society in which virtually all human behavior may be monitored, tracked and analysed, and selectively 'nudged' in certain directions – ranging from Fitbit's exhortations of greater physical fitness,[5] to Pandora's music recommendations,[6] to Facebook's mood manipulation experiment,[7] to

---

* Professor of Law, Melbourne Law School, University of Melbourne.

[1] Defining the Sensor Society conference, University of Queensland, 8-9 May 2014.

[2] Smart Cities Forum, Victorian Privacy and Data Protection Commission, Melbourne, 9 May 2016.

[3] Thanks especially to Rachelle Bosua, Karin Clark and Jeb Webb, collaborators with on a Melbourne Networked Society Institute-Melbourne Law School funded project on the Internet of Things 2015-2017 for suggestions and ideas that contributed to this article.

[4] Cf Mark Andrejevic and Mark Burdon, 'Defining the Sensor Society' (2015) 16 *Television & New Media* 19.

[5] See David Pogue, *Wearable Devices Nudge You to Health* (26 June 2013) New York Times (Online) <http://www.nytimes.com/2013/06/27/technology/personaltech/wearable-devices-nudge-you-to-a-healthier-lifestyle.html?_r=0>.

[6] See Cass Sunstein, *Choosing Not to Choose* (Oxford University Press, 2015) 109.

[7] See Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment: It was probably legal. But was it ethical?* (8 September 2014) Atlantic Monthly (Online) <http://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>.

Pokémon Go bringing players out on the streets,[8] to CCTV cameras employed in smart cities to monitor and reduce crime, to numerous targeted advertisements exhorting us to buy more and more things. Moreover, as people's personal data is held potentially indefinitely by numerous so-called trusted collectivities which may not, as it turns out, be quite so trustworthy, there is a risk of unexpected and unwanted revelation by third parties over whom the data subjects (being a step removed) seem to have minimal control. Indeed massive data loss is increasingly viewed as an inherent risk of a modern data-driven agency or organisation's activities. And the question now is whether and where we might want to draw a legal line on these diverse activities, taking into account all of their various benefits and costs.[9]

The benefits are agreed to be wide-ranging, yielding improvements in terms of services, efficiency, innovation, health and welfare, to name a few.[10] But it is tempting to characterise the costs simply in terms of a generic loss of 'privacy' (or risk thereof). For instance, Daniel Solove in an important article defines the harms to privacy that may occur in contemporary society as embracing both a mixture of loss of control over the processing of personal information and invasions into people's private affairs.[11] Others talk in terms of 'data privacy', or 'information privacy', as covering the first part of Solove's generic definition, *viz*, control over the processing of personal information.[12] But I want to argue that interests in privacy are more properly characterised in terms of Solove's second (more traditional and precise) category of invasions into private affairs.[13] As to the first category, these interests, which have to do with bureaucratic processes of information storage, handling and use, may be better conceived as coming under a general rubric of data protection or, as the

---

[8] Mark Weinberger, *The CEO behind 'Pokémon Go' explains why it's become such a phenomenon* (12 July 2016) Business Insider <http://www.businessinsider.my/pokemon-go-niantic-john-hanke-interview-2016-7/?op=1?r=US&IR=T#5kTHCBFi7TSIjfwy.97>.

[9] Cf Jules Polonetsky and Omar Tene, 'Privacy and Big Data: Making Ends Meet' (2013) 66 *Stanford Law Review* 25, 26 ("Finding the right balance between privacy risks and big data rewards may very well be the biggest public policy challenge of our time").

[10] See Carol Saab, 'The Ingredients (and our Vision) for a Smart Society' on *CSIRO Blog* (20 July 2015) <https://blog.csiro.au/the-81st-ranking-that-we-want-to-change/>.

[11]Daniel Solove, *The Meaning and Value of Privacy: Appeal for a Pluralistic Definition of the Concept of Privacy* (23 April 2010) OPEN Magazine <https://www.onlineopen.org/download.php?id=20>. And see generally Solove's book, *Understanding Privacy* (Harvard University Press, 2008).

[12] Presumably that is what Polonetsky and Tene, above n 9, have in mind in using the language of 'privacy' to characterise the risks associated with big data.

[13] Solove suggests that this category includes 'invasive acts that disturb one's tranquility or solitude' and incursions into a data subject's decisions regarding her private affairs: *The Meaning and Value of Privacy*, above n 11, 5. Another category of invasion into private affairs might be publications that disclose a person's private affairs to others (being circumstances which may also disturb one's tranquility): see *PJS v News Group Newspapers Ltd* [2016] UKSC 26 (19 May 2016) [26] and [35] (Lord Mance), [58]-[59] (Lord Neuberger).

German Constitutional Court puts it,[14] 'informational self-determination'.[15] Further, neither of these categories quite captures one of the most general concerns about pervasive monitoring of humans – a concern about surveillance as an exercise in power which, whether for benign or for malign purposes, effectively disempowers the subject.[16] And there may be another concept worth noting here, also having to do with human agency – an idea about consumer and citizen empowerment, which holds that individuals should be able to make informed and independent choices about the way they conduct their lives in a democratised market-based society.[17] In other words, if the benefits of our networked and increasingly automated society are multiple and various then so (I argue) are the risks, or costs. Or, if there is one general label to be employed here, it has to do with a broad idea of individual dignity, autonomy and personhood rather than a somewhat quaint and antiquated sounding idea of 'privacy'.[18]

II REGULATORY RESPONSES

The reasoning suggests that a mix of regulation may be the best response to the risks (or costs) noted above. For instance, if one concern is about the potential for observation/scrutiny deployed as a technique of power then the regulatory solution may be to ensure that the monitoring is conducted with proper authority, limits and oversight – as with the various Australian *Surveillance Devices Act*s which have provisions about who is entitled to engage in surveillance through the deployment of surveillance devices and on what terms.[19] Further, if another concern is with the ways that personal data may be

---

[14] Bundesverfassungsgericht [German Constitutional Court], 1 BvR 209/83, 15 December 1983 reported in (1983) 65 BverfGE 1 ('Population *Census Case'),* translated and noted in Donald Kommers and Russell Miller, *The Constitutional Jurisprudence of the Federal Republic of Germany* (Duke University Press, 3rd ed, 2012) 408.

[15] Although, appreciating that this is a rather purist position to adopt, especially in Australia, I concede that 'data privacy' may be a practical compromise label to use for this category

[16] See David Lyon, *The Electronic Eye: The Rise of Surveillance Society - Computers and Social Control in Context* (Wiley, 2013) ch 4.

[17] Cf Sunstein, above n 6, 7 – giving examples of choices about "health care, romance, marriage, financial markets, consumer protection, poverty, the availability of organs, energy use, environmental protection, obesity, mortgages, savings", and so on. In broad terms these can be understood as consumer or democratic choices.

[18] The idea that the right to privacy is a nineteenth century idea is one I explore further in my book *The Right to Privacy: Origins and Influence of a Nineteenth Century Idea* (Cambridge University Press, 2017 [forthcoming]).

[19] *Surveillance Devices Act 2004* (Cth); *Surveillance Devices Act 2007* (NSW); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA); *Listening Devices Act 1992* (ACT); *Surveillance Devices Act* 2007 (NT). For an overview and recommendation that these Acts should be dealt with in a more streamlined uniform fashion, see Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014) ch 14.

systematically collected, processed and stored (the computerised database is a standard trope here), then the answer may be to subject these processes to the fair data management standards of data protection laws looked after by a data protection commissioner – as with the Australian *Privacy Act 1988* (Cth),[20] loosely modelled on OECD and European Data Protection standards,[21] and the more appropriately termed *Privacy and Data Protection Act 2012* (Vic).[22] Consumer protection standards may also play a role in dealing with concerns about informed consumer choice – and we already have provisions in the Australian Consumer Law which might effectively be deployed against misleading and otherwise unfair trade practices as well as product liability standards for products, or things, that fail to meet consumer expectations.[23] It may fairly be argued that a degree of 'messy multi-valence' is desirable here (for instance, in the same way that in the absence of a generalised US data protection law consumer protection law is used in the United States to provide a degree of effective data protection,[24] the same should occur in Australia for those organisations which fall under the $3 million annual turnover 'small

---

[20] *Privacy Act 1988* (Cth), as amended by the *Privacy Amendment (Private Sector) Act 2000* (Cth) (extending the Act to organisations) and *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (introducing reforms including a new set of Australian Privacy Principles in response to recommendations of the Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008). And see further, for the latter applied to big data, Office of the Australian Privacy Commissioner, *draft Guide to Big Data and the Australian Privacy* Principles (2016) Office of the Australian Information Commissioner <https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/>.

[21] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980) [updated 2013]; *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281/31. The first is noted in the preamble to the *Privacy Act 1988* (Cth), while the second is noted indirectly in the reference to the object of "meet[ing] international concerns and Australia's international obligations relating to privacy", in s 3 of the *Privacy Amendment (Private Sector) Act 2000* (Cth).

[22] *Privacy and Data Protection Act 2014* (Vic). See also *Information Privacy Act 2014* (ACT); *Privacy and Personal Information Protection Act 1998* (NSW)*; Invasion of Privacy Act 1971* (Qld); *Information Privacy Principles Instruction (IPPI) 1989* (SA)*,* published as Premier and Cabinet Circular No 12 (reissued 2016); and *Personal Information and Protection Act 2004* (Tas); and generally Office of the Australian Information Commissioner, *Other Privacy Jurisdictions* <https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions>.

[23] *Competition and Consumer Act 2010* (Cth), sch 2 ('*Australian Consumer Law*') (with mirror legislation in the states and territories), especially ss 18 (misleading or deceptive conduct), 21 (unconscionable conduct in connection with goods or services) and 138 (Liability for loss or damage suffered by an injured individual).

[24] In particular, *Federal Trade Commission Act,* 15 USC § 45(a) (1914). (Section 5, unfair or deceptive acts or practices): see Chris Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (Cambridge University Press, 2016).

business' exception in the *Privacy Act*[25]). No doubt the laws could be further updated and improved – for instance drawing on the techniques of automation to set standards of 'data protection by design', as provided for in the new EU Data Protection Regulation.[26] But, in terms of their broader goals, they remain surprisingly relevant to contemporary policy concerns.

On the other hand, when the concern is about privacy, it may not be enough just to rely on generalised data protection, surveillance or consumer protection standards. For even if these other laws may sometimes provide a degree of effective protection to privacy,[27] there are still cases where laws need to be more individually focussed and judged, using doctrines that are framed around privacy – including in cases involving high degrees of automation. For instance, in the recent English case of *Vidal-Hall v Google* the plaintiffs discovered that Google's 'Safari workaround' had managed to bypass the Apple Safari firewall to target advertisements on their Apple device. They argued that Google had breached the *Data Protection Act 1998* (UK), misused their private information under the UK privacy tort, and breached their confidence. In proceedings about service out of jurisdiction, the trial judge allowed the first two claims to go forward, leaving out the third only on the basis that there was no provision for service out of the jurisdiction for an equitable claim,[28] and his decision was upheld on appeal.[29]

Interestingly, when it came to the argument about misuse of private information, Google's suggestion that Apple users were only being 'observed' by its technology in order to collect and analyse and make use of their data to advertise (so in a sense they remained 'anonymous') was rejected by the judge

---

[25] See Privacy Act 1988 (Cth), ss 6C-6EA – and note this was an exemption that the Australian Law Reform Commission recommended should be removed in its 2008 report, above n 20, recommendation 39.

[26] European Parliament and Council (2016), *Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1, art 25.

[27] Especially in respect of sensitive personal information, such as health information, typically accorded higher protection under data protection regimes (including under the Australian *Privacy Act*) – and see *Z v Finland* (1997) 25 EHRR 371 [95] (the European Court of Human Rights noting that "the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the [European Convention on Human Rights] (art. 8).").

[28] *Vidal-Hall v Google, Inc* [2014] 1 WLR 4155, upheld on appeal.

[29] *Google, Inc v Vidal-Hall* [2015] FSR 25 (27 March 2015). Leave to appeal to the Supreme Court on other grounds dealt with in the judgment in *Google, Inc v Vidal-Hall* (on the question of damages for emotional distress under the Act, taking into account the terms of the Directive and the EU Charter rights) was granted on 28 July 2015, but withdrawn on 1 July 2016: see *Vidal-Hall v Google Goes to the Supreme Court* (1 July 2016) Carter-Ruck <http://www.carter-ruck.com/news/read/vidal-hall-v-google-goes-to-the-supreme-court>.

on the basis that individual third party observers could easily become involved, including those who might incidentally observe the advertisements in a shared office environment.[30] Further, while the case could also be dealt with under general data protection standards,[31] the privacy claim was treated as a more particular claim about the use of certain private information (with further details provided in confidential schedules submitted by the claimants), suggesting that 'privacy' here was seen as something more individual than just having to do with personal data, or personal information.

III PRIVACY AS AN INDIVIDUALISED INTEREST

In other words, privacy still seems to be a highly individualised interest, deeply inculcated with personal values. This may imply a poor fit with the idea of an automated society. Yet this is the traditional view of privacy. So when Samuel Warren and Louis Brandeis talked about the right to privacy as a right to be 'let alone' in their 1890 *Harvard Law Review* article,[32] their concern was privacy as a highly individualised interest, securing "to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others".[33] Similarly, on the other side, their concern was with the "too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds" on "the privacy of the individual".[34] And their recommendation was for a new privacy tort to supplement the (individualised) protection that was already available in the hands of judges under more traditional doctrines such as breach of confidence. The reasoning seems to presuppose a high level of individual involvement at all steps of the process, from plaintiff to defendant to judge.

But is this necessarily precluded by an automated society? Already we can see from the *Vidal-Hall* case that the plaintiffs had privacy sensitivities about targeted advertisements (with more detail in the confidential schedules), that Google Inc. were seen as responsible at some level for the deliberate bypassing of Apple Safari security measures to target advertisements to these individuals using their private information, and that a particular concern was that there were human audiences which might be made privy to this information. For

---

[30] *Vidal-Hall v Google, Inc* [2014] 1 WLR 4155 [115]-[120].

[31] Or in the US under the *Federal Trade Commission Act,* 15 USC § 45 (1914), with Google paying $22.5 million to settle the charges: see Federal Trade Commission, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (9 August 2012) <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>.

[32] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

[33] Ibid 198.

[34] Ibid 206.

another example we might turn to the earlier case of *Peck v United Kingdom*[35] where footage of Geoffrey Peck attempting suicide in the High Street in Brentwood, Essex, was later shown on local and national television at the instigation of the Brentwood Borough Council (in an effort to demonstrate the effectiveness of the technology in saving his life). Peck successfully argued that the Council's conduct amounted to violation of his private life, in breach of Article 8 of the European Convention on Human Rights.[36] The court agreed, underlining the Council's lack of sensitivity in exposing one of the darkest moments of Peck's life for public view. The decision effectively signalled to agencies and organisations that when decisions are made about the exposure of a person's sensitive information (as in that case in advertising the success of the Council's CCTV technology without taking the minimal step of adequately masking Peck's face), the decision-makers involved should be mindful of the likely effect on the person's sense of their privacy. It may help to think that certain types of information are "obviously private", as Gleeson CJ said in *Australian Broadcasting Corporation v Lenah Game Meats*, giving examples of "health, personal relationships, or finances".[37] But *Peck* and *Vidal-Hall* suggest that what is required is a more individual, human assessment by the putative privacy infringer of the putative privacy subject's personal characteristics, along with the information and other relevant circumstances, to ascertain whether the activity will breach that person's sense of privacy – an assessment required also of the judge if a case comes to court.

In short, assessments of privacy are not susceptible (at least as yet!) to an automated solution – and, when it comes to issues of law reform, doctrines framed in terms of privacy, with standards arbitrated by judges in court,[38] would still seem to be a desirable approach.

---

[35] *Peck v United Kingdom* (2003) 36 EHRR 41.

[36] *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).

[37] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 226 [42] (Gleeson CJ).

[38] As recommended inter alia by the Australian Law Reform Commission, above n 19; Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the Serious Invasion of Privacy in New South Wales* (2016); South Australian Law Reform Institute (2016); South Australian Law Reform Institute, *A Statutory Tort for Invasion of Privacy*, Final Report 4 (2016). See further Megan Richardson, 'Reforming Privacy Law – Again!' (2013) 5 *Journal of Media Law* 345.

The Trouble with Using Search Engines as the Primary Vector of Exercising the Right to be Forgotten

Stuart Hargreaves*

ABSTRACT

European privacy law currently implements the 'right to be forgotten' by positioning commercial search engine operators as the initial site of decision-making regarding its exercise. This is problematic for a number of reasons. First, there are a number of structural flaws in the mode of this decision-making that make it unclear that search engines are capable of (or interested in) incorporating a robust account of competing interests. Second, right to be forgotten requests are not susceptible to the same kind of algorithmic techniques search engines use to deal with other kinds of removal requests, meaning large numbers of decisions must be made rapidly and primarily by staff lacking formal legal qualifications. When compounded with the possibility of heavy penalties for failure to comply with the right under European law, these two issues suggest there is a significant potential for bias toward deletion rather than preservation of borderline links. A third problem is that the simple online forms provided by search engines for European data users making a deletion request mask a complicated legal analysis, meaning those who properly structure their requests in an appropriately technical and legal manner may have a higher chance of success in their claims. This threatens to open up a new digital divide along the axis of reputation. Finally, the massive compliance costs associated with this new right may serve as a form of anti-competitive lock-in, preventing the emergence of innovative new companies in 'search'. In sum, if the right to be forgotten is to have real meaning in European law, search engines are not the correct vector for its implementation.

I INTRODUCTION

A so-called 'right to be forgotten' has gained significant traction in recent years within both the privacy community and the broader public consciousness.

* Assistant Professor, LLB Programme Director and Assistant Dean (Undergraduate Studies), Faculty of Law, Chinese University of Hong Kong.

Conceptually, it draws heavily from a longstanding right in the civil law known as *le droit a l'oubli*, or 'the right of oblivion'. The importance of rehabilitation is the root of this right: having paid their debt to society by serving a particular punishment and then being released, effective rehabilitation meant criminals deserved a 'fresh start' and ought not to be confronted with their past errors at every turn.[1] Translated into legal terms, this right of oblivion meant that information about those crimes could not be republished absent some compelling reason. But even in jurisdictions that did not formally recognise such a right, the practical difficulty of accessing and searching archives of news stories in the pre-digital era meant that for the vast majority of people past errors would eventually fade from public consciousness. The twenty-first century, of course, presents a very different reality: the shift of news media to the internet along with the development of search engines that can comb through and index databases, blogs, and websites of all kinds in the blink of an eye has changed this entirely. And not, of course, just for criminals. A life lived significantly online – as is the case for billions of people around the world – means leaving digital footprints that are no longer washed away by the tides of time, but rather serve as indelible markers of our presence and our actions. As Mayer-Schonberger argues, the internet means that a "default of forgetting" has shifted towards a "default of remembering";[2] new claims for recognition of a right to be forgotten can be interpreted in large part as a response to this shift. The broad strokes of the normative arguments both in favour of and against the right to be forgotten have been well-covered in the literature,[3] and I do not intend to go over that ground again here. Instead, this article considers the difficulties posed by the particular *form* that the right has taken in European privacy law, as represented first by the CJEU's 2014 elucidation in *Google v González*[4] and then by its subsequent explicit inclusion in

---

[1] Jeffrey Rosen, 'The Right to Be Forgotten' (2012) 64 *Stanford Law Review Online* 88, 88.

[2] Victor Mayer-Schonberger, *Delete: the Virtue of Forgetting in a Digital Age* (Princeton University Press, 2009).

[3] See, eg, Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Data Practice' (2011) 8 *Scripted* 229; Napoleon Xanthoulis, 'The Right to Oblvion in the Information Age: A Human-Rights Based Approach' (2013) 10 *US-China Law Review* 84; Cecile de Terwangne, 'Internet Privacy and the Right to be Forgotten / Right to Oblivion' (2012) 13 *Revista de internet, derecho y politica* 109; Jef Ausloos, 'The 'Right to be Forgotten' -- Worth Remembering?' (2012) 28 *Computer Law & Security Review* 143; Alessandro Mantelero, 'The EU Proposal for a General Data Protection Regulation & the Roots of the 'Right to be Forgotten'' (2013) 29 *Computer Law & Security Review 229*; Jeffrey Rosen, 'The Right to be Forgotten' (2012) 64 *Stanford Law Review Online* 88; Jeffrey Rosen, 'The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google' (2012) 80 *Fordham Law Review* 1525; Michael L Rustad and Sanna Kulevska, 'Reconceptualising the Right to be Forgotten to Enable Transatlantic Data Flow' (2015) 28(2) *Harvard Journal of Law & Technology* 349; Simon Wechsler, 'The Right to Remember: The European Convention on Human Rights and the Right to be Forgotten' (2015-2016) 49(1) *Columbia Journal of Law & Social Problems* 135.

[4] *Google Spain v AEPD and Mario Costeja González* (C-131/12) [2014] ECJ 317 ('*González*').

the General Data Protection Regulation,[5] scheduled to come into force in 2018. Though formal routes of appeal to national data protection authorities (DPAs) and the judicial system are preserved, both these articulations of the right nonetheless envision search engines as the primary deciders of any claim. This raises at least four problems.

First, the decision-making processes adopted by search engines in order to give effect to the right to be forgotten do not appear to lead to a particularly robust account or defence of the public interest or other competing values. A private organization with commercial interests at its heart is left to determine which information is properly 'remembered' for the benefit of the public. Second, the vast number of deletion requests received by search engines poses a significant challenge. While search engines are able to automate (at least initially) removal of links to copyrighted material or child pornography through the use of digital 'thumbprints', the same techniques cannot apply to complicated decision-making that must balance off a variety of legal rights. When combined with the possibility of heavy penalties under the GDPR for failure to give proper effect to the right, these first two problems are likely to lead to a bias on the part of search engines towards deletion rather than preservation of 'borderline' links. Indeed, Google's own statistics (*infra*) indicate that the relative rate of deletion is increasing. The third problem relates to the process an individual must complete before a search engine agrees to remove links. It is both relatively technical and 'legalistic', and this may mean that the right is more easily accessible by those with the resources to hire 'reputation management' companies or those who are digitally-savvy; those lower on the socio-economic scale or who are ignorant of how the internet works may find this new right does comparatively little for them, opening up a new digital divide along the axis of reputation. Finally, the costs of compliance with the right to be forgotten by search engines – especially if they take the right seriously and create procedures designed to minimize the first three problems I have identified – may in fact be so high as to result in competitive 'lock-in'. By this, I mean that the current dominant players in 'search' may be the only ones who can afford the compliance costs associated with the right to be forgotten, thus limiting the possibility of new entrants. As currently envisioned, then, implementation of the right to be forgotten primarily through reliance on search engines has serious weaknesses.

[5] *Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119 ('GDPR').

II THE RIGHT TO BE FORGOTTEN IN EUROPEAN LAW

The primary vehicle for the protection of personal privacy in European law, the European Data Protection Directive,[6] does not contain an explicit right to be forgotten, though it does contain a number of rights related to erasure of personal data or cessation of further processing. Art. 6(1)(a), for instance, requires that all data collection and processing must be done "lawfully". Art. 6(1)(c) provides that "personal data must be… adequate, relevant, and not excessive" given the original purpose of collection or processing, while Art. 6(1)(d) adds that data that is inaccurate or incomplete must be "erased or rectified". Art. 12(b) guarantees the right of every data subject to obtain "rectification, erasure, or blocking of data" if its processing fails to comply with other provisions of the Directive, with a particular emphasis on the ability to exercise the right if the data is "inaccurate or incomplete". With regard to the cessation of further processing, Art. 14 allows a data subject to object to processing on "compelling legitimate grounds", particularly if the legal justification under Art. 7 for processing is not the consent of the data subject but rather the "legitimate interests" of the data controller. Of course, the Directive does not create *absolute* rights of personal control over one's data. In addition to numerous broad exceptions to the entire Directive, Art. 13, for instance, allows EU Member States to restrict the scope of the rights and obligations found in both Arts. 6 and 12 if necessary "to safeguard… the rights and freedoms of others." Likewise, the requirement that the grounds of objection under Art. 14 be "compelling" and "legitimate" also implies that the right to object to further processing is not absolute.

Though it has been the touchstone law regarding the personal privacy of Europeans for the last twenty years (and a global model for data protection regimes),[7] the Directive was drafted and enacted prior to the emergence of algorithms that relentlessly crawled the web, indexing it and drawing connections between disparate pages and subsequently presenting links to end users upon the input of certain keywords; in other words, before anyone knew what a 'search engine' was. How, then, should the Directive apply in the context of search engines? Are search engines data controllers? That is, do they collect or process personal information when they index a webpage created by a third party and then provide a link to it in response to the user input of certain search terms? If so, what is the legal justification for that processing? When a search engine links to a webpage with outdated information, are they

---

[6] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281/31 ('Directive').

[7] Stuart Hargreaves, 'Data Protection Regimes' in Christopher Anglim (ed), *Privacy Rights in the Digital Age* (Grey House Publishing, Inc, 2016) 133.

violating Art. 6(1)(d)? Can a data subject ask for deletion from a search engine of a link to a website that contains their personal information under Art. 12(b)? On what grounds? If linking itself is a kind of processing, can a data subject object to further processing under Art. 14? If the answer to any of the above is yes, what is the impact of competing rights of free expression or access to information? All these questions, *inter alia*, were considered in *González*.

III GONZÁLEZ V GOOGLE

In 1998, the Spanish newspaper La Vanguardia Ediciones published a story[8] regarding the court-ordered sale of the private property of Mario González as a result of his unpaid debts.[9] A decade later, González was no longer a debtor and was disheartened to discover that when he typed his name into Google, a link to an online version of the newspaper announcement was one of the top results. Initially, he contacted La Vanguardia and requested that they delete the story from their website. They declined, so he turned his attention to Google. In 2010, he wrote to Google's Spanish subsidiary requesting deletion of any links to the story and also made a formal complaint to the Spanish Data Protection Agency (*Agencia Española de Protección de Datos* – AEPD) about both the existence of the newspaper story online and Google linking to it. He requested an order that La Vanguardia remove the relevant pages or obscure his details and that Google delete any relevant links to the information, on the grounds that "the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant."[10] The AEPD rejected his complaint regarding La Vanguardia, finding that publication was "legally justified as it took place upon the order of the Ministry."[11] However, it upheld González' complaint against both Google Spain and its US parent, Google Inc., finding that the Directive gave the AEPD the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense.[12]

Google Spain and Google separately appealed to the National High Court (Audiencia National), which joined the actions and then stayed pending answer

---

[8] 'Story' is perhaps a bit generous – the newspaper was required to print it and similar announcements by the Ministry of Labour and Social Affairs in order to increase the likelihood of the government recovering the unpaid debts by selling off the properties.
[9] *González* (C-131/12) [2014] ECJ 317 [14].
[10] Ibid [15].
[11] Ibid [16].
[12] Ibid [17].

from the CJEU on the following three main questions (plus a variety of sub-questions) regarding the proper interpretation of the Directive:

1. What are the requirements for a search engine to be considered as 'established' within the meaning of Art. 4(1)(a)?
2. Is a search engine a 'data controller' that 'processes' personal data within the meaning of Arts. 2(b) and (d)?
3. Does the Directive establish a 'right to be forgotten' through Arts. 12(b) and 14(a)?[13]

The CJEU rendered its decision in May of 2014, accepting that the business plan of targeting Spanish users through keyword advertising was sufficient to invoke the application of the Directive. The Court found that a search engine meets the requirements of Art. 4(1)(a) (that is, the data processing at issue is 'carried out in the context of the activities of an establishment of the controller on the territory of a Member State') if the search engine "intended to promote and sell, in the Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable."[14] The CJEU also found that there was no meaningful difference between Google Spain SL and Google, Inc. It was irrelevant, said the CJEU, that the 'seat' of the search engine was outside the EU, since the "activities of the operator… and those of its establishment situated in the Member State… are inextricably linked."[15]

The CJEU also found that search engines were "processing data" within the meaning of the Directive:

> in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results… must be classified as 'processing' within the meaning of [Art. 2(b)].[16]

---

[13] Ibid [18]-[20]. The interpretive questions regarded the EU Data Protection Directive since Spain had chosen to incorporate it directly through the Organic Law 15/1999 rather than implementing it through national legislation.
[14] Ibid [55].
[15] Ibid [55]-[56].
[16] Ibid [28].

The Court also found that search engines met the definition of 'data controller', concluding that they "determine the purposes and means of that activity and thus of the processing of personal data", and so "must be regarded as the 'controller' in respect of that processing."[17] To exclude search engines from the definition of 'data controller' simply because they do not control the content of third party webpages would, in the Court's view, have been entirely contrary to both the wording and the objective of Art. 2(d).[18] This was because search engines played a "decisive role in the dissemination" of personal data, making it accessible to any internet user who typed in the data subject's name.[19] Since search engines enabled users to "establish a more or less detailed profile of the data subject", the Court concluded they were "liable to affect significantly… the fundamental rights to privacy and protection of personal data."[20] The Court rejected the claim that existence of robots.txt[21] flags or other similar exclusionary tools meant that search engines could not be data controllers, finding that the protection of the Directive for data subjects was not waived simply because a third-party webpage host declined to use such a tool.[22] Thus, they concluded, when indexing the web and generating links to in response to keywords, search engines ought to be considered as 'data controllers' that 'processed' data within the meaning of Art. 2(b) and (d).

Did a data user, then, have the right under the Directive to request a search engine remove links from a list of results that were displayed upon entry of their name? The Court noted first that any processed data had to comply with the quality requirements laid out in Art. 6, which held that if data were inaccurate or incomplete, then a data processor was under an obligation to rectify or delete it. But a search engine, of course, did not control the content it linked to. This implied then that any 'deletion' in the context of search engines would be limited to the removal of links to the information. A second path to deletion might be found through Arts. 7 & 12. Art. 7 lists the possible legal justifications for processing, such as the explicit consent of the data subject or that it is necessary in order to complete a contract to which the data subject is a party. The Court argued that search engines could only rely on Art. 7(f), which permits processing where necessary for the legitimate interests of

---

[17] Ibid [32]-[33].
[18] Ibid [34].
[19] Ibid [36].
[20] Ibid [37]-[38].
[21] Robots.txt and similar tools allow webmasters to indicate to search engine algorithms that they do not wish their pages to be archived, indexed, or otherwise included in the search engine's records. Though algorithms are not forced to respect these flags, as a matter of practice the major commercial search engines do. For more see, *About /robots.txt*, The Web Robots Page <http://www.robotstxt.org/robotstxt.html>.
[22] *González* (C-131/12) [2014] ECJ 317 [39].

the controller or the third parties to whom the personal data is disclosed, unless these interests are overridden by the interests and rights of the data subject. [23] This latter clause meant that proper application of Art. 7(f) required a balancing exercise between opposing rights.[24] Failure of a data controller to establish a valid justification under this Article (either by failing to identify a legitimate interest or by failing to strike the right balance) would allow the data subject to obtain deletion through Art. 12(b). While not strictly the same as deletion, data subjects could also object to further processing of their data by reference to Art. 14(1)(a), which allowed them to lodge objection to the processing on "legitimate grounds relating to [their] particular situation." This too, said the Court, involved a "balancing" question, but allowed a more specific consideration of the data subject's factual need, rather than broader interests and rights.[25] The Court also concluded that requests from a data subject either for removal under Art. 12(b) or for cessation of further processing under Art. 14(1)(a) could be submitted directly to the relevant data controller; if the controller denied the request, only then could the data subject could bring the matter to the relevant national DPA or judicial body.[26] It was here that the CJEU first selected search engines as the primary vector of the exercise of the right to be forgotten, and it is from here that many later difficulties flow.

Of critical import under either a deletion request under Art. 12(b) or a cessation of processing request under Art. 14(1)(a) is whether the processing strikes the appropriate balance between the rights of the data subject and the interests of the data controller or third parties. In *González*, the CJEU concluded that given "the potential seriousness of the interference" with the privacy rights of the data subject, the economic interests of the search engine operator could not alone justify continued processing against the former's will.[27] The Court accepted that removal of links could also impact upon the legitimate interests of other internet users, but found that as a "general rule" the data subject's rights would override them, "depending on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information."[28] What, then, was the fair balance between these rights?

---

[23] Ibid [73]-[74].
[24] Ibid [74].
[25] Ibid [76].
[26] Ibid [77].
[27] Ibid [81].
[28] Ibid.

The CJEU argued that the balance tilted toward the data subject where:

> [I]nitially lawful processing of accurate data [becomes] in the course of time… no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.[29]

Thus, if a data subject submits a request for deletion under Art. 12(b) and it can be shown that the list of links provided by a search engine in response to a query involving her name contains links to webpages that contain personal data that despite being true and originally lawfully published, if having regard to all the circumstances of the case is now "inadequate, irrelevant, or no longer relevant", then she may obtain removal of those links;[30] less a right to be forgotten, then, and a more a right to be 'de-listed'.

The CJEU accepted this implicated important countervailing interests, but nonetheless believed that only in rare instances would the right of the public to receive information override this right of the data subject; for instance, if the data subject played a particular role in public life.[31] On the particular facts before them, the CJEU found that "there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of a search, access" to the information regarding González's earlier financial difficulties (though the final decision would ultimately be that of the referring court, of course).[32] The court found there was no obligation upon La Vanguardia, however, to delete the old story from its website or otherwise modify its content to eliminate mention of González. In so doing, the Court set up the strategic primacy of the search engine as the site for the exercise of right to be forgotten claims from the perspective of the data subject. As the original source of the information, a newspaper is much more likely to push back in a robust defence of their competing right to free expression or the access rights of the public. A search engine does not have the same responsibility or need to preserve content, and so is a smarter target for a data subject seeking to mask certain information.

---

[29] Ibid [93].
[30] Ibid [94].
[31] Ibid [97].
[32] Ibid [98].

IV ART 29 WP GUIDELINES ON THE RIGHT TO BE FORGOTTEN

Several months after the release of *González*, the Article 29 Data Protection Working Party released a set of Guidelines on the proper implementation of the decision by national DPAs.[33] The Working Party said data subjects were free to make such requests to either a search engine or an original content hosting site, since they were both data controllers (though with two different legitimating grounds for the processing in which they engage – search engines fall under Art. 7(f)). But accepting the reality established by the CJEU, which had clearly anticipated that a challenge to an original webhost rather than a search engine would be substantially less likely to succeed, the Working Party paid special attention to search engines, arguing that "data subjects should be able to exercise their rights with search engine operators using any adequate means [including but not limited to] online procedures and electronic forms."[34] Search engines, the Working Party said, were free to request identification from an applicant, along with specifics regarding the links applicants were seeking to have erased, their justification for seeking deletion, and information about any role they fulfilled in public life.[35] The Working Party also noted that in the case of a valid request, search engines were not required to *delete all links* to the relevant page, but rather simply not *show* links to a particular website when the identified individual's name (or variant) was inputted into the search box.[36] The Guidelines concluded that though a balance between the privacy rights of the individual and the free expression rights of others or the public's general right to access information had to be struck, "in practice the impact of de-listing on individual's rights to freedom of expression and access to information will prove to be very limited."[37]

However, though it had earlier in the document acknowledged that search engines would be the likely recipients of deletion requests, the Working Party nevertheless said it would fall *to the DPAs* to "systematically take into account the interest of the public in having access to the information"; if the interest of the public overrode the rights of the data subject, then de-listing would not be appropriate.[38] So, even though the Working Party assumed that search engines might create procedures to allow individuals to request deletion/hiding of

---

[33] *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain Inc. v. AEPD and Mario Costeja González" C131/12, Article 29 Data Protection Working Part* [2014] 14/EN WP 225 <http://ec.europa.eu/justice/data-protection/article-29/documentation /opinion-recommendation/files/2014/wp225_en.pdf> ('The Guidelines').
[34] The Guidelines, 13.
[35] Ibid 14.
[36] Ibid 21.
[37] Ibid Executive Summary 3.
[38] Ibid.

particular links, it appears to have also believed that the DPAs would be responsible for the heavy analytical lifting. To that end, the Working Party created a set of criteria as a "flexible working tool" to help DPAs during their decision-making process.[39] There was no single determinative criterion, but "each [had] to be applied in the light of the principles established by the CJEU and in particular in the light of the 'interest of the general public in having access to the information.'"[40] These included questions regarding the role (if any) a data subject played in public life, whether the data subject was a minor, whether the data was accurate, whether it was irrelevant or excessive, whether it was sensitive, the context in which the data was published, etc. These are all reasonable and important questions. However as I will shortly demonstrate, rather than being asked by the DPAs in the method seemingly envisioned by the Guidelines, they have ended up being asked by search engines and ultimately this proves problematic.

V THE RIGHT TO BE FORGOTTEN UNDER THE GENERAL DATA PROTECTION REGULATION

The judgment in *González* occurred parallel to an ongoing multi-year review of the Directive by the European Commission; after several years of discussion and negotiation, the Member States agreed to a final text of the GDPR, in force from May 2018. The need to replace the Directive is made clear in the Recital to the GDPR:

> Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally.[41]

To address these challenges, the GDPR has a number of features that distinguish it from the Directive, the first of which is simply its mode of implementation. In European law, a 'Regulation' is directly applicable in every Member State whereas a 'Directive' can be implemented by Member States in a number of ways. This means the GDPR should significantly improve

---

[39] Ibid part II: List of common criteria for the handling of complaints by European data protection authorities.
[40] Ibid.
[41] *GDPR*, recital 5-6.

harmonisation of data protection laws across Europe, making compliance easier for companies that operate across borders. Substantively, key features include an extension of the law to include *all* foreign companies who process the personal data of EU residents for the purposes of offering goods or services to those residents, even if those companies are not headquartered in the EU and the processing occurs outside the EU.[42] There are new mandatory breach notification requirements that mean a company that suffers a data loss must report it to a national DPA within 72 hours.[43] There is a new right to data portability, allowing users to bring their personal data with them from one commercial service to another.[44] There are new, harsher penalties for failure to comply with the requirements of the GDPR.[45] And most importantly for the purposes of this paper, the 'right to be forgotten' is explicitly introduced:

> A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject.[46]

Art. 17 of the GDPR provides for the new right to be forgotten as a component of the previous right of erasure, in a fashion that is largely consistent with the principles outlined in *González*. Under the new law, a data subject has the right to obtain erasure from a data controller "without undue delay" where, *inter alia*, the data is no longer necessary to fulfil the purposes of collection, where consent is withdrawn if consent was the original justification for processing, or where the data subject objects under Art. 21 to further processing of any personal data the collection or processing of which was initially justified by the legitimate interests of the controller or third party.[47] In the context of search engines, it is this latter route that would most likely provide the ground for exercising a data subject's right to be forgotten, since search engines that automatically index the web and generate links to it do so without the explicit consent of the data subject. If a data subject objects under Art. 21 to further processing in this way, then the burden shifts to the data controller to prove that there are "compelling legitimate grounds" for the processing to continue that override the data subjects rights.[48] If there are no such grounds, then Art. 17 provides that the data must be erased. The GDPR does not refer to 'de-listing', but rather refers to 'deletion' or 'erasure' of

---

[42] Ibid art 3(2). This is, of course, consistent with *González*.
[43] Ibid art 33.
[44] Ibid art 20.
[45] Ibid art 83.
[46] Ibid recital 65.
[47] Ibid art 17(1).
[48] Ibid art 21(1).

personal data. However, it is reasonable to conclude that erasure or deletion in the context of search engines continues to mean de-listing; since *González* was released prior to the final draft of the GDPR, had the Commission wanted to revisit the question of de-listing as a form of erasure or to exclude search engines from the meaning of 'data controller' they had the chance to do so. It is notable though that the language of "inadequate, excessive, or irrelevant" found in *González* was not adopted – instead, the question is simply a balancing off of competing interests. On the other hand, given that the GDPR places the burden upon the data controller to demonstrate 'compelling legitimate grounds' to override the data subject's rights, it is reasonable to assume that the overall approach to this balance taken by the courts in *González* (that is, presumptively in favour of the data subject) will remain.

The GDPR also introduces a new concept of 'restriction of processing'. Under Art. 18, a data subject can request immediate restriction of further data processing where an objection has been lodged under Art. 21, pending verification of the claim.[49] 'Restriction' can also be requested by the data user under Art. 18 if they would have a right to erasure under Art. 17 but would prefer that the information not be permanently erased. According to the Recital, 'restriction' can be achieved by "making the selected personal data unavailable to users, or temporarily removing published data from a website."[50] This provision also seems well suited for the idea of 'de-listing' of links in response to particular search terms, though its use as such has yet to be tested in court. The GDPR further requires that where a data controller has made personal information public and is now subject to a right to be forgotten request, they must take all reasonable steps to inform other controllers that are processing the data that the subject has requested erasure of the data, including links to or copies of that data.[51] This means, for instance, that if a data subject were able to obtain the right to be forgotten as against a website hosting their personal data, that website would then be obliged to inform search engines to also delete relevant links to or caches of the original page – no separate application would be necessary. All the rights contained in Art. 17, however, do not apply to the extent that the processing is necessary "for exercising the right of freedom of expression and information."[52] Thus, the balancing question can be addressed at multiple levels of the legal analysis, though it remains to be seen if it will be interpreted by the courts in a different manner depending at which point it is introduced.

---

[49] Ibid art 18(1)(d).
[50] Ibid recital 67.
[51] Ibid art 17(2).
[52] Ibid art 17(3)(a).

The new regulation also contains measures to ensure effective and rapid implementation of the right upon request by the data subject. Under Art. 12, the right to be forgotten is included in the rights a data controller "shall facilitate", and must act upon without "undue delay, and in any event within one month of receipt of the request."[53] Access to this right must be provided "free of charge", however controllers may refuse to act upon or charge a fee for "manifestly unfounded or excessive" requests, "in particular because of their repetitive character."[54] However, failure of the data controller to respect any of the rights outlined in Arts. 17 and 18 can lead to harsh penalties, including administrative penalties of 20 million euros or up to 4% of total worldwide annual turnover, whichever is higher.[55]

VI THE PROBLEMATIC RELIANCE ON SEARCH ENGINES AS THE FIRST-ORDER 'DECIDERS'

In sum, these changes mean that though the wording of the GDPR does not identically match the form of the right elucidated by the CJEU in *González*, in the context of personal information processed by a search engine its application appears largely the same – a search engine will be considered a data controller under an obligation to either erase (Art. 17(1)) or restrict access to (Art. 18(1)) links to otherwise legally published personal information if a data subject objects (Art. 21(1)) to further processing of that information, unless the controller can show that there are legitimate grounds (Arts. 17(3), 21(1)) that override the privacy rights of the data subject. Though the GDPR indicates that a right to be forgotten claim can be made against either the original publisher *or* a search engine, the ability of a data subject to obtain de-listing of multiple links through a single request to a search engine means that search engines are likely to remain the primary vector for the exercise of this right. In the sections that follow, then, I want to outline some concerns that stem from placing this burden upon search engines. The first of these relates to the decision-making process applied by search engines when considering a request to remove or mask a link under the rubric of the 'right to be forgotten'. Google, for instance, provides European data subjects wishing to exercise the right with a simple web form to complete, which includes the links/pages requested for deletion, the name of the data subject, the justification for deletion, etc. Google says they use a four-part procedure to evaluate requests "in accordance with" the Article 29 Working Party's Guidelines (*supra*):

[53] Ibid arts 12(2) and (3).
[54] Ibid art 12(5).
[55] Ibid art 83(5).

1. Does the request contain all the necessary information for us to be able to make a decision?
2. Does the person making the request have a connection to a European country, such as residency or citizenship?
3. Do the pages appear in search results for the requester's name and does the requester's name appear on the page(s) requested for delisting?
4. Does the page requested for removal include information that is inadequate, irrelevant, no longer relevant, or excessive, based on the information that the requester provides? Is there a public interest in that information remaining available in search results generated by a search for the requester's name?[56]

Given Google's direct reference to the Guidelines, it is reasonable to assume that they are also using the criteria outlined in Part II of the Guidelines when it comes to answering their fourth question, which is of course the most challenging one. Though Microsoft does not make explicit reference to the Guidelines in its removal tool for Bing Search, the information it asks for appears relatively similar, with an online form for data subjects seeking removal of links that asks for identification information, the link in question, and whether the data subject is "a public figure" or has a "role in [their] local community or more broadly that involves leadership, trust, or safety (for example teacher, clergy, community leader, police, doctor, etc.)."[57] It is also reasonable to assume, then, that Microsoft also relies on the Guidelines when trying to respond to right to be forgotten requests. Yahoo too makes no direct reference to the Guidelines, but does state that removal will be done in accordance with the criteria outlined by the CJEU. Its removal request form asks for identification, the link, "an explanation", and a check-box that certifies the applicant has no "honest and reasonably held belief [of a] conflict with the general public's right to know about the information" sought to be de-listed.[58] Since Yahoo Search is powered by Bing Search,[59] it stands to reason that its removal methodology likely also adheres to the Guidelines.

---

[56] *FAQ – European Privacy in Search*, Google Transparency Report <https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en>.
[57] *Request to Block Bing Search Results in Europe*, Bing, Webmaster Tools <https://www.bing.com/webmaster/tools/eu-privacy-request>.
[58] *Requests to Block Search Results in Yahoo Search: Resource for European Residents*, Yahoo <https://uk.help.yahoo.com/kb/search/sln24378.html>.
[59] Greg Sterling, *Yahoo-Bing Reach New Search Deal* (16 April 2015) Search Engine Land <http://searchengineland.com/yahoo-bing-renegotiate-search-deal-yahoo-gains-right-to-serve-search-ads-on-the-pc-219020>.

But this is problematic. As noted, the Working Party explicitly described the criteria contained in the Guidelines as being for the reference of *DPAs* in determining if the public interest should overrule a right to delisting on a case by case basis, not search engines. The criteria are therefore designed for consideration by a quasi-judicial body, not a commercial organisation. For example, in considering whether a 'public figure' or someone having a 'role in public life' may nonetheless retain a privacy interest over certain kinds of private information, the Guidelines encourage DPAs to make reference to *von Hannover v. Germany (No. 2)*, which attempted to draw a distinction :

> between reporting facts capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their official functions, for example, and reporting details of the private life of an individual who does not exercise such functions.[60]

In considering de-listing in the case of minors, the Guidelines instruct DPAs to consider the concept of the "best interests of the child", as explained by a body of jurisprudence relating to Art. 24 of the EU Charter of Fundamental Rights.[61] When considering the question of whether the data is relevant and not excessive (bearing in mind of course that this may no longer be a consideration under the GDPR), the Guidelines suggest the overall purpose of this question is to "assess whether the information contained in a search is relevant or not according to the interest of the general public in having access to the information", and this might relate to the age of the information, whether it constitutes hate speech/slander/libel, whether it appears to be a personal opinion or a verified fact, etc.[62] The Guidelines also ask whether the data processing is causing prejudice to the data subject, or whether it has a disproportionately negative privacy impact on the data subject (tautologically, the Guidelines go on to suggest that it is disproportionate if there is no wider public interest in the availability of the information).[63] These are but a subset of the questions and examples the Guidelines offer to help a DPA try and determine the existence of whether there is an overriding public interest in the information. My argument is that a search engine, whether it is Google or Bing or another competitor, is ill-placed to answer many of them.

The Guidelines were designed for quasi-judicial or administrative bodies such as a DPA, whose *raison d'etre* is to consider the balance and interaction of

---

[60] The Guidelines, part II, 2, citing *von Hannover v. Germany (No. 2)* (2012) 55 Eur Court HR 15.
[61] Ibid part II, 3.
[62] Ibid part II, 5.
[63] Ibid part II, 8.

privacy rights and other rights in their national implementations of the Directive or the GDPR. Search engines are profit-making corporations whose primary duty in law is to their shareholders; putting them in the position of deciding what is in the public interest is therefore illogical and unwise. They should not be imputed with the decision-making capacity of a DPA. The relative opacity of their processes – they are not open in the way a judicial hearing would be, nor do they publish detailed explanations of their decisions so that they can be reviewed – means we do not know how the public interest is advocated for during internal discussions, or whose freedom of expression the search engine might be concerned about. Are they worried about their own freedom of expression in terms of their ability to link, or are they concerned about the free expression of third party webpages in terms of their ability to reach a wide audience by being indexed? Are they worried about the ability of the public to access information for its own sake, or are they worried about the commercial perception of their business depending on what they choose to remove? In short, there is no strong or clearly identifiable advocate of competing interests other than those of the search engine when these decisions are made, and no public record of how they are reached – we simply have to rely on good faith that the public interest and the rights of others have been taken into account. In contrast, the data subject can forcefully and personally advocate to the search engine exactly *how* their interests are harmed by the continued processing of the information, meaning there is more likely to be a compelling case presented for deletion rather than preservation.

This disparity in effective representation is compounded because an 'appeal'[64] from an internal decision by a search engine to delete or preserve a link is in practice available to only one party – the data subject. If a data subject requests a link be removed by a search engine and the search engine complies, there is no entity representing 'the public interest' that can then appeal the decision to a national DPA or judicial authority. Only in cases where the subject of the request is already particularly well-known might, for instance, a newspaper make a request to a DPA that a search engine's decision be reversed. But in such circumstances, it is less likely that the search engine would have deleted the link in the first place, since the data subject in question may have some 'role in public life'. For the vast majority of requests, then, no party will be present to appeal on behalf of the public for continued access to the information at issue. Indeed, a decision to delete may never become publicly known and is in such cases, in practice if not law, 'final' – Google's annual 'transparency report', for instance, simply describes in general terms a subset of requests they have processed in the previous year; there is no

[64] By this I mean of course the possibility of challenging the decision of the search engine in some manner, rather than a formal appeal from a legal decision.

comprehensive database of all requests made and the results. But if a data subject's claim is rejected, they may still apply directly to their national DPA, and from there, into the judicial system. Though the right of 'appeal' from a decision of a search engine is available to all, in practice it is primarily only going to be exercised by a data subject whose request has been rejected. A search engine wishing to avoid the possibility of litigation that is expensive, time-consuming, or unwanted from a public relations perspective may therefore lean towards deletion rather than preservation in the case of borderline links. There are thus a range of structural factors that suggest search engines are likely to either be unable or unwilling to strongly advocate for the public interest in deliberations when deciding whether to preserve or remove links, particularly if they are seen to be 'borderline' in nature.

A second problem with reliance on search engines as the primary vector of the exercise of the right to be forgotten stems from the massive number of requests for removal they receive. Google and Bing have both developed algorithms that help them automate large numbers of requests for removal of links to things like copyrighted material or child pornography. Such material is susceptible to an initial (if imperfect) detection through machine learning – algorithms can essentially 'thumbprint' certain materials and identify copies wherever they are online. This allows, for example, Google to remove thousands of instances of copyrighted material on YouTube with relative ease. Now, this has proven to be problematic in its own right, insofar as the technique may automatically remove material that is under copyright but is nonetheless legitimately being used in the service of parody, fair comment, education, etc.[65] But it still allows Google to cut down the number of cases that must be subsequently reviewed by human eyes to something more manageable. Interpreting 'right to be forgotten' requests is, however, a far more complicated endeavour that is not susceptible to the same machine learning techniques. Proper implementation requires a complicated balancing off of the privacy rights of the data subject against the free expression or access to information rights of the public; this is not something that can be decided algorithmically. Yet, the numbers of requests faced by search engines are staggering. In the first five months following the release of *González*, Google alone received approximately 145 000 separate requests regarding

[65] See, eg, Maayan Perel and Niva Elkin-Koren, 'Accountability in Algorithmic Copyright Enforcement' (2016) *Stanford Technology Law Review* (forthcoming); Peter S. Menell, 'Google, PageRank, and Symbiotic Technological Change' (Research Paper No 2136185, UC Berkeley Public Law, 2012); Laurie Cubbison,'False Positives Reveal Problems with Copyright Enforcement Software' (March 2013) 8 *The CCCC-IP Annual: Top Intellectual Property Developments of 2012* 26; Benjamin Boroughf, 'The Next Great Youtube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation' (2015) 25 *Albany Law Journal of Science and Technology* 95.

almost 500 000 links, of which it ended up deleting roughly one-third.[66] From when it launched its website tool for European users wishing to make a request for deletion (May 2014) to the time of writing (July 2016), Google has received over half a million requests, regarding 1.6 million separate links, of which it has removed 43%.[67] This works out to an average of between 650 to 700 new requests per day, with each of those requests containing reference to an average of three or four distinct links. Assuming one request takes a *minimum* of 30 minutes to properly review, a dedicated reviewer working 8 hours a day could get through no more than 8, suggesting a requirement of a full-time staff of approximately 125 (assuming they each work 8 hours a day, 5 days a week) just to initially review the requests. Google says 30% of requests are escalated to senior staff and attorneys, implying the initial decision to delete or reject is taken by compliance staff with no formal legal qualifications.[68] Google does not provide an explanation of how the junior staff decide to escalate. Are all links marked initially for deletion escalated? The reverse? It is unclear. But given the speed with which junior staff must make a decision, the ever-increasing number of requests, and the difficulty of identifying with clarity the public interest given a lack of dedicated legal training, there remains a significant risk of bias towards deletion rather than preservation. Indeed, it is notable that when Google first released statistics about how it dealt with right to be forgotten requests, it indicated it agreed to approximately one-third of them, but now that number is approaching nearly half.[69]

Both of these issues – the structural or institutional difficulties in properly considering the public interest in preservation of links and the challenge of effectively processing a massive flood of removal requests – are compounded by the heavy penalties that can befall a search engine under the GDPR (again, up to 4% of worldwide turnover). In 2015, Google's worldwide revenue was approximately USD 75b, implying a theoretical penalty for violation of the right to be forgotten of up to USD 3b. Now, it is unlikely that such a stringent penalty would be levied in all but the most flagrant of privacy violations, however it nonetheless indicates the financial risks a company runs if they fail to properly comply with the requirements of the GDPR. These risks may also increase bias towards deletion rather than preservation of certain kinds of personal data; it is safer and easier for a search engine to delete rather than preserve seemingly 'borderline' links. Of course, excessive deletion of links

---

[66] Jo Best, *Google grants one-third of 'right to be forgotten requests* (10 October 2014) ZDnet <http://www.zdnet.com/article/google-grants-one-third-of-right-to-be-forgotten-requests/>.
[67] *European privacy requests for search removals*, Google Transparency Report <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en>.
[68] *Who makes decisions to delist content?*, European Privacy in Search FAQ <https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en>.
[69] Best, above n 66; above n 67.

means that significant amounts of information about data subjects will, for most practical purposes, be scrubbed from easy access by the public, whether or not that individual becomes someone with a public role *at some point in the future*. There is no automatic expiry of the right to be forgotten in the future, or some systematic way for us to know which people will be of interest or which events in their life the public would benefit from scrutinizing at some point in the future. Thus, even a moderate bias towards deletion rather than preservation may have a dramatic impact upon the right of public access to information that simply may not be apparent to (or even capable of being appreciated by) the search engines tasked with the initial decision.

A third problem raised by reliance on search engines as the first-order 'deciders' of the validity of any given removal request also relates to the mechanics of the process. The typical process, as outlined, involves a data subject inputting a relatively limited amount of information into an online form – identification, the link in question, the reason for the deletion request, whether they have some public role, etc. But the apparent simplicity of the forms may mask from most users a complicated legal question implicated by every request. For many, the reason for seeking removal may simply be "it's embarrassing" or "I don't like it" – after all, the mass media narrative surrounding the right to be forgotten presented it essentially as the right to remove information about yourself from the internet that you did not want there. There was relatively little discourse in the media about what impact that might have on competing interests or how they could be weighed. It is reasonable to anticipate that a staff member is more likely to agree to a deletion request when it is packaged clearly, articulated properly, and made with reference to the relevant legal principles. Thus, it is likely that those who have the resources to craft their requests in appropriately legal or technical phrasing will have a substantially increased chance of success. Indeed, the online forms created by both Google and Microsoft anticipate that removal requests may come from not only the data subjects themselves, but also from 'authorized representatives'. Unsurprisingly, a range of commercial services have sprung up to fill this role and to smooth the passage of any given request.[70] I have already identified possible bias towards deletion rather than preservation; the effects of this bias would only be aggravated if deletion of 'borderline' links were more easily achieved by some socio-economic groups than others. In effect, it would risk the creation of a new digital divide along the axis of reputation, in which some are able to scrub their history from public view and others are not. For all the problems that the right to be forgotten may pose for free expression rights and the public's right to access

[70] Sam Frizell, 'There's a 'Right to be Forgotten' Industry – and It's Booming', *Time* (online), 18 July 2014 <http://time.com/3002240/right-to-be-forgotten-2/>.

information, if it is to apply it must at a minimum apply equally to all as a matter of *practice*, not simply as a matter of *law*.

The fourth problem associated with using search engines as the main drivers of the right to be forgotten again relates to the massive number of requests received. Due to the difficulty in automating these requests, as explained, there are significant staffing requirements associated with complying with the law. Google is far and away the dominant player in 'search', and so it currently has to deal with the highest number of requests for deletion and therefore probably faces the most significant compliance costs as a result. But the impact of these costs may go far beyond Google's bottom line. What if, for instance, a new search engine were launched in a garage in Palo Alto, or a university classroom in Bangalore, or in a shared workspace in Shenzen? What if this new search engine were radically more effective than Google, such that it rapidly supplanted it and became the new 'default', in the way that Google rapidly supplanted Lycos, AltaVista, and the other search engines that predated it? Should this new search engine offer services to anyone in the EU, it would have all the same compliance obligations as any other data controller. But technology start-ups rarely have a significant staff size, and certainly cannot afford large numbers of non-revenue generating compliance personnel until they are well-established. Search engines, by their very nature, process and index quantities of information orders of magnitude greater than traditional kinds of data controllers, and so will be subject to remarkably high labour costs if they are to comply with European privacy law. The burden of compliance with the right to be forgotten may therefore be a kind of anti-competitive lock-in, preventing the emergence of new competitors to Google, Bing, et al.

VII CONCLUSION

In this paper I have tried to separate out the question of whether or not the 'right to be forgotten' is a good thing from whether or not an expectation that search engines will be the primary vector for exercising that right is a good thing. I have suggested it is not, for at least four reasons. First, there are structural and procedural difficulties with the decision-making process of the search engines that mean there is unlikely to be forceful advocacy for the public interest or other countervailing rights to those of the data subject. Second, I question whether search engines have the labour capacity to truly deal with massive numbers of right to be forgotten requests in a way that properly takes into account the complicated balancing of rights and interests that must occur. When these two problems are combined with the possibility of significant penalties for breach of the GDPR, I argue that prudence on the part of search engines will create a bias towards deletion rather than preservation of 'borderline' links. Indeed, early evidence suggests that (at least

in the case of Google) the rate of deletion as a percentage of requests received is increasing. Third, the technical or legal know-how required to craft an effective removal request may mean that those with access to certain resources will be more easily able to scrub certain kinds of information about them from the internet, opening up a new kind of 'digital divide' along the axis of reputation. Finally, the costs of compliance associated with applying the right to be forgotten to search results may serve as a kind of anti-competitive lock-in, preventing the emergence of competitors and innovation in the search engine industry.

What then, is the solution? Prior to releasing its decision in *González*, the CJEU sought the Opinion[71] of the then Advocate General of the EU, Niilo Jääskinen. Jääskinen's Opinion[72] offered a different perspective on the role of search engines than the one ultimately chosen by the Court, one that is in my view more logical. Unlike the Court, he argued that though Google was indeed processing data when its algorithms indexed billions of pages across the web, it ought not to be treated as a 'data controller' within the meaning of the Directive. The definition of a 'data controller' in the Directive, to recap, is "a natural or legal person… which alone or jointly with others determines the purposes and means of the processing of personal data."[73] As does the recital of the GDPR, the Advocate General noted that the Directive was effectively a 'pre-internet' document, and so it

> did not take into account the fact that enormous masses of decentrally [sic] hosted electronic documents and files are accessible from anywhere and that their contents can be copied and analysed and disseminated by parties having no relation whatsoever to their authors or those who have uploaded them onto a host server connected to the internet.[74]

Jääskinen argued that the intent of the Directive was to create responsibility for controllers over personal data when they were aware the data they were processing contained personal information and intentionally did so *because* it was personal data, for their benefit.[75] In contrast, he said, an:

> internet search engine service provider merely supplying an information location tool does not exercise control over personal

---

[71] A common practice when the Court is confronted with a novel point of law.
[72] *Google Spain SL Google Inc.v Agencia Española de Protección de Datos (AEPD)Mario Costeja González* (Case C-131/12) {2013} 424 (Advocate General Jääskinen) ('*The AG Opinion*').
[73] Directive, art 2(d).
[74] *The AG Opinion* (Case C-131/12) {2013} 424 [78].
[75] Ibid [83].

> data included on third-party web pages. The service provider is not 'aware' of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. In the course of processing of the source web pages for the purposes of crawling, analysing and indexing, personal data does not manifest itself as such in any particular way.[76]

Since a search engine had no ability to modify or delete the content on the third party webpages, it therefore lacked the "locus of factual influence" which determined where the responsibility of compliance with the Directive lay.[77] Search engines, for instance, index webpages that may include special categories of personal information such as political opinions or health data that, under the Directive, require the express consent of the data subject before processing can occur. To treat search engines as data controllers in such circumstances would have the effect of making all search engines illegal under European law, a conclusion that, as Jääskinen said, would be "absurd."[78] If the Court had agreed with the Advocate General, then search engines would not have been tasked with being the first-order deciders of any data subject's claim to a right to be forgotten, since they would not have been considered "data controllers" within the meaning of the law.

This analysis is eminently sensible, and is based upon an acceptance of important distinctions between the different operations that a search engine undertakes. There is an obvious difference between processors of information that do so intentionally and for the purpose of identifying individuals or to market services to them based on a profile, and those that do so incidentally in the service of another goal. Now, to be sure, search engines do process personal data *qua* data controllers at times – Google, for example, attempts to serve data subjects particular advertisements based on information they have collected and processed about them. There is no question that a data subject should have the right to request that a search engine delete any such information gained about them through the data subject's use of their services or by tracking their actions across multiple websites through persistent cookies. This should not be controversial and is a sensible approach to the right to be forgotten. But this is very different than the kind of incidental processing of personal information that occurs when a search engine simply points to the existence of lawfully published information elsewhere on the web and temporarily caches snapshots of those websites in order to serve previews of them to users. Search engines conduct different kinds of information-

[76] Ibid [84].
[77] Ibid [88].
[78] Ibid [89]-[90].

related operations within the broader concept of 'search', and it is a mistake to conflate the two. Unfortunately, both the CJEU's approach to the right to be forgotten in *González* and the Commission's approach to it under the GDPR appear to do just this.

While the right to be forgotten may have value, it is nonsensical to expect search engines to be the primary vector of that right – it not only misunderstands the way in which information is processed in the context of an internet search, but places a burden upon search engines which, as I have argued in this paper, they cannot properly shoulder. If the EU strongly believes in the importance of creating a genuine right to be forgotten rather than a half-way house of a right to be 'de-listed', then logically it should be targeted at the primary hosting websites or publishers of the personal information in question. Such a system would provide for a significantly greater chance for countervailing interests to be properly represented. A primary host, for instance, has a far greater incentive to represent its own free expression interests than does a search engine. But a proper balance could still be achieved, since even if a host rejected a request, then a data user would still be free to bring a claim to a competent authority such as a DPA, who would then choose whether or not to order the primary data controller to erase the information. That decision would still be made on the basis of whether it had been shown that the right of free expression of the host or the access to information rights of the public outweighed the privacy rights of the data subject. If a primary data controller were ordered to delete information by a DPA, they would then be under an obligation to notify search engines to delete any links or caches to that original information in order to give effect to the data subject's right to be forgotten. Only if a search engine refused to remove that cache or link would the DPA have to step in and order de-listing. This process would no doubt be more cumbersome from the perspective of the data subject, and would probably greatly reduce the number of successful requests. But it would take more seriously the countervailing rights of both the public and third parties in a way that the current implementation of the right to be forgotten in European law, which places a commercial entity with profit at its heart as the primary vector for its exercise, does not.

International Cybercrime Investigations and Prosecutions: Cutting the Gordian Knot

Marie-Helen Maras*

Cybercrime challenges the security and stability of countries by transcending traditional borders and having an international impact. Because cybercrime often involves more than one jurisdiction, collaboration between countries in the investigation of this illicit activity is required. Such cooperation between countries was observed in Operation Shrouded Horizon. This operation involved the investigation of Darkode, an online password-protected site, which sold illicit goods and services (e.g. malware), and stolen data (e.g. personal and financial data).[1] This site operated by invitation only and required new members to be sponsored and vetted by existing members of the forum. The investigation of Darkode involved 19 countries and resulted in the arrest of approximately 70 members of the forum and their associates from various countries around the globe.[2] Operation Shrouded Horizon is by no means unique; it is highlighted here as a case study to illustrate the importance of countries working together on cybercrime cases.

Despite successful cooperative investigations, such as Operation Shrouded Horizon, barriers to international cybercrime investigations and prosecutions remain. Cybercrime cannot be effectively investigated and prosecuted if the countries involved do not have adequate and harmonised national cybercrime laws and enforcement mechanisms, and lack the national capacity needed to investigate and prosecute cybercrime. This article briefly explores these obstacles, looking in particular at those resulting from the absence of enforcement and lack of harmonisation of cybercrime laws, the differences between countries' digital forensics practices and rules of evidence, and the current national deficit in digital forensics expertise and ability to conduct and/or assist in international cybercrime investigations and prosecutions.

---

* Associate Professor, Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice.

[1] United States Federal Bureau of Investigation, *National Cyber Security Awareness Month* (1 October 2015) <https://www.fbi.gov/news/stories/national-cyber-security-awareness-month>.

[2] Daniel Victor, *Authorities Shut Down Darkode, a Marketplace for Stolen Personal Data* (15 July 2015) *New York Times* (online) <http://www.nytimes.com/2015/07/15/technology/authorities-shut-down-darkode-a-marketplace-for-stolen-personal-data.html?smprod=nytcore-ipad&smid=nytcore-ipad-share&_r=0>.

I CYBERCRIME LAWS: THE CASE FOR ENFORCEMENT AND HARMONISATION

Multilateral and regional treaties, agreements, and conventions exist which relate to cybercrime. An example of a multilateral convention is the 2001 Council of Europe's *Convention on Cybercrime*, which sought to remove obstacles to effective and efficient cybercrime investigations by establishing mechanisms that foster international cooperation in cybercrime cases.[3] Regional agreements and conventions have also been implemented that govern cooperation between countries on matters relating to cybercrime and cybersecurity. Examples of such agreements and conventions are the:

- 2001 Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information;
- 2009 Shanghai Cooperation Organisation Agreement on Cooperation in the Field of Information Security; and the
- 2010 League of Arab States Arab Convention on Combating Information Technology Offences.

Despite the existence of multilateral and regional treaties, agreements, and conventions, there continue to be obstacles to cooperation between countries in international cybercrime investigations and prosecutions. Certain countries are not members of these treaties, agreements, and conventions, and even those that are parties to them may not have the necessary infrastructure and human and financial resources to cooperate with other countries in cybercrime investigations. Moreover, countries that are parties to these treaties, agreements, and conventions may be incapable, reluctant or unwilling to cooperate with other parties.

Accordingly, these multilateral and regional treaties, agreements, and conventions while a step in the right direction, are not all that is needed to successfully investigate and prosecute cybercrime. What is also needed is the effective enforcement of these treaties, agreements, and conventions, and national cybercrime laws. Furthermore, harmonised national cybercrime laws are needed to enable the investigation and prosecution of cybercrime and prevent the existence of cybercrime safe havens.

---

[3] *Convention on Cybercrime*, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004).

II VARIATIONS IN DIGITAL FORENSICS PRACTICES AND RULES OF EVIDENCE

Due to the pervasiveness of Internet-enabled technologies in day-to-day activities of individuals around the globe, a wealth of digital data can be gleaned from these devices, which could be used as evidence in cybercrime prosecutions. The evidence needed to effectively prosecute a cybercriminal may reside in a different jurisdiction (or different jurisdictions) than the location of the perpetrator and/or victim (or victims). As such, the issue primarily lies not with the availability of data (which resides on the digital device, with few exceptions), but with the ability of criminal justice agents to access, collect, and preserve digital evidence[4] in a manner that would ensure its admissibility in a court of law.

Computer forensics (or digital forensics) professionals acquire digital devices, and identify, evaluate, and preserve digital evidence for use in legal proceedings, which can be used to prove or disprove the commission of a cybercrime, crime or policy violation.[5] To ensure the admissibility of digital evidence in a court, a lawful search must be conducted and the chain of custody[6] must be maintained. What is more, digital evidence must be authenticated before it can be used in legal proceedings. Authentication seeks to establish the integrity of evidence (i.e. evidence is what it purports to be and has not been modified in any way). Because digital evidence is volatile and can be manipulated, digital forensics professionals must prove that what is being introduced in court has not been altered.[7]

Ultimately, to be admissible in court, digital evidence must meet the evidentiary requirements of the court in the jurisdiction where the case is being tried. These requirements are stipulated in national rules of evidence. National rules of evidence govern the introduction and use of different types of evidence in a court of law. National rules of evidence differ between countries, even those with similar legal traditions. In the context of digital

---

[4] Digital (or electronic) evidence is "any type of information that can be extracted from computer systems or other digital devices and that can be used to prove or disprove an offense or policy violation." Marie-Helen Maras, *Computer Forensics: Cybercriminals, Laws and Evidence* (Jones and Bartlett, 2nd ed, 2014) 38.

[5] Ibid 29.

[6] The chain of custody includes detailed information about who obtained the evidence, when and where the evidence was obtained, how it was obtained, and anyone who accessed the evidence and for what reasons it was accessed.

[7] For example, if systems and devices from which evidence is obtained have weak access control and authentication measures (e.g. anti-virus and anti-spyware programs, and passwords), the integrity of the evidence may be called into question because the data is at risk of manipulation from, for example, malware and hackers.

forensics, these rules determine what digital evidence can be collected and the manner in which it should be collected and preserved in order to ensure its admissibility in court.

Countries use formal and informal mechanisms to share digital evidence. The formal mechanisms used to request and share evidence and information relating to cases being investigated include mutual legal assistance treaties (MLATs),[8] letters rogatory,[9] and multilateral, regional, and bilateral agreements.[10] Informal mechanisms include police to police cooperation between countries. Digital evidence obtained through informal channels may be deemed inadmissible in a court due to differing rules of evidence between countries, lack of harmonised digital forensics practices between countries, and issues with the chain of custody.[11]

III NATIONAL CAPACITY DEFICIT

The transnational element of cybercrime further complicates digital forensics. Accessing digital evidence is difficult and often depends on the relationships between the requesting country and the country providing the assistance, and the national cybercrime laws and capabilities of the country where the evidence resides. In fact, one of the greatest hurdles to overcome is the current deficit in national capacity in countries around the world to conduct cybercrime investigations and prosecutions.

Criminal justice agents with the necessary knowledge, skills, and abilities to investigate and prosecute these crimes, as well as the funds, equipment, and facilities, are needed. Knowledge of the type of digital evidence that can be gleaned from digital devices and that which is needed to prove that a crime was committed is essential. Given the vast range of digital devices (e.g. smartphones and gaming consoles), services (e.g. cloud storage), and new technologies (e.g. Internet of Things[12] devices), criminal justice agents and

---

[8] Mutual legal assistance treaties are "agreements between countries that dictate the type of assistance provided by each nation in criminal investigations (e.g., with respect to evidence and resources), and for the extradition of cybercriminals." Marie-Helen Maras, *Cybercriminology* (Oxford University Press, forthcoming) 78.

[9] Letters rogatory are "used to request evidence from other countries. These letters include information about the case, a description of the evidence needed and why it is needed, and a promise for reciprocity in future cases." Ibid.

[10] Marie-Helen Maras, *Transnational Security* (CRC Press, 2014) 144-145.

[11] The evidence obtained from a country through informal channels may not meet the evidentiary standards of the requesting country.

[12] The Internet of Things (IoT) connects individuals, animals, plants and everyday objects to the Internet, enabling their real-time surveillance, and the acquisition, archiving, analysis, and sharing of vast quantities of data about them in order to provide some service. For more information

other digital forensics professionals need continuous training to keep abreast with advances in the field, and digital technology, apps or other software that may interfere with investigations and prosecutions. The reality is that the technical and legal expertise to conduct cybercrime investigations and prosecutions is not widely available; the technical expertise for criminals to conduct cybercrime is. Cybercriminals may or may not have the necessary knowledge, skills, and abilities (KSAs) to conduct cybercrime. This, however, does not serve as a limiting factor; cybercriminals without these KSAs can purchase goods and services online to enable them to commit cybercrime.[13] Specifically, hacking and malware services that are "made to order" are available for purchase online.[14]

The deficiencies in national capacities to conduct cybercrime investigations and prosecutions were revealed in a 2013 United Nations Office on Drugs and Crime (UNODC) report.[15] Particularly, this report revealed that countries had a critical shortage of criminal justice agents with the necessary KSAs and lacked the financial and technical resources (e.g. digital forensics tools and equipment) that were needed to adequately investigate and prosecute cybercrime. This not only limits these countries' ability to investigate and prosecute cybercrime within their own countries, but also prevents them from being able to assist other countries with their cybercrime investigations and prosecutions. Countries that are unable to conduct cybercrime investigations and prosecutions because of these limitations may receive outside assistance from international organisations (e.g. UNODC and Interpol) and other countries. This outside assistance, however, only serves as a temporary fix to the present national deficit.

To build national capacity, digital forensics academicians and professionals should travel to countries in need and provide comprehensive training to criminal justice agents and others in the field of digital forensics. Those trained will then train others in the field. Notwithstanding, this training, like the assistance that international organisations provide to countries in need, only works in the short term. To truly deal with the deficit, the education requirements for criminal justice agents and police academy curricula should change. Individuals entering into the field of criminal justice, law, and law

---

on the Internet of Things, see Marie-Helen Maras, 'The Internet of Things: Security and Privacy Implications' (2015) 5(2) *International Data Privacy Law* 99.

[13] For further information on illicit goods and services sold online, see Maras, above n 8, Ch 11.

[14] For example, a cybercriminal can request a specific type of malware online, which will be created for him or her for a fee.

[15] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (Report, February 2013) <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_ STUDY _210 213.pdf>.

enforcement should have a basic working knowledge of computers, information technology, and digital forensics. Furthermore, given that few geographic areas and aspects of individuals' daily lives have been left untouched by Internet-enabled digital technologies, it is safe to assume that non-specialised law enforcement officers (i.e. those who are not trained in digital forensics) will come in contact with digital devices during their investigations; as such, police academy curricula should be modified to include the basic information officers need to understand these devices and how to handle them.[16] Initiatives such as these are essential to improving digital forensics training for non-specialised law enforcement and other criminal justice agents.

IV THE SOLUTION

Current approaches to international cybercrime investigations and prosecutions can be viewed as an attempt to detangle the Gordian knot.[17] Greek accounts of the Gordian knot claimed that all attempts to detangle the Gordian knot proved futile.[18] The best approach to dealing with the Gordian knot was to cut it – as Alexander the Great did. To cut the Gordian knot (i.e. to efficiently and effectively deal with the current obstacles in international cybercrime investigations and prosecutions), a multifaceted approach is required:

- National laws and international treaties, agreements, and conventions should be harmonised and adequately enforced;
- Digital forensics practices and rules of evidence should be harmonised around the globe to prevent the existence of cybercrime safe havens and enable the successful prosecution of cybercriminals; and
- National capacity in digital forensics should be strengthened.

These changes can improve cooperation in international cybercrime investigations and prosecutions, enabling countries to work together on common threats they face (irrespective of where the cybercrime took place), which adversely impact them as sovereign nations.

---

[16] Maras, above n 10, 148.

[17] In Greece, an oracle prophesised that the individual who untied the Gordian knot in Phrygia would become the king of Asia. Many tried to untie the knot but failed because the knot was impossible to unravel. Alexander the Great cut the knot with his sword. See Brendan Burke, 'Anatolian Origins of the Gordian Knot' (2001) 42 *Greek, Roman, and Byzantine Studies* 255.

[18] See ibid.

Private Lawmaking in Commercial Cyberspace

Eliza Mik*

No discussion of "Law and Technology" would be complete without at least one essay centred on the Internet. While the Internet no longer captures our imagination with the same force as it did 20 years ago, we cannot assume that it no longer creates (or *perpetuates*?) multiple legal problems. When we talk about the Internet we must, however, refrain from the popular "Internet meta-narrative" that often leads to superficial arguments and unhelpful generalisations.[1] We must always remain aware of the multiplicity of the Internet's *technical* applications and the wide range of *legal* contexts in which the term gains significance. Discussing the Internet in the context of freedom of speech or cybercrime raises different legal issues than in the context of commerce or contract. In most instances, we should avoid mentioning the Internet altogether and refer to specific Internet-enabled technologies or services, such as the web or video streaming. This brief essay addresses one specific issue: the regulation of online activity by means of private agreement. I have, however, chosen yet another term to provide the backdrop for the discussion: "cyberspace." Although we know that cyberspace only exists at some esoteric, conceptual level,[2] I have chosen the term to pay homage to early cyberspace scholarship, to invoke the reader's memories of its idealistic values and its promotion of separatist, self-regulatory thinking. Consequently, embellishing cyberspace with the adjective "commercial" seems highly inappropriate, if not heretical. After all, cyberspace is supposed to be free, permeated with community spirit and libertarian values. How can it be *commercial*?

We must, however, acknowledge the changed character of the Internet and therefore, unavoidably, cyberspace. Neither the Internet nor the web can still be referred to as novel or revolutionary. Internet-based technologies, ranging from email to mobile apps, have become permanently integrated into our everyday lives. The Internet is used for professional and personal communications, for entertainment, for public services, politics and religion. More importantly, the Internet has become commercial. To explain: the first phase of commercialisation of the Internet was associated with the development of network infrastructure, the sale of networking products, and basic connectivity. This phase related to the *privatisation* of the Internet, to the

---

* Assistant Professor of Law, School of Law, Singapore Management University.

[1] Evgeny Morozov, *To Save Everything Click Here* (Allen Lane, 2013) 18.

[2] Julie E Cohen, 'Cyberspace as/and Space' (2007) 107 *Columbia Law Review* 210, 213.

move from the state-funded NSFNET backbone to the long-distance, high-capacity networks provided by commercial operators. The second phase of commercialisation can be associated with technological developments aimed at providing new services that use the Internet as a transmission infrastructure, such as the distribution of digital content (e.g. Amazon, Netflix) or the provision of cloud-based services (e.g. Gmail, Facebook, Dropbox). More specifically, the web is used to access mass media (television, radio, newspapers) as well as many forms of digitised entertainment (films, music, books). Consequently, although we associate the web with freedom of expression and political activism, its practical role is often reduced to that of an access interface to online resources.

In sum, contrary to popular beliefs, the Internet economy is a capitalist economy.[3] And the main tool of regulating commercial exchanges in capitalist economies is contract. While we need not debate whether contract law continues to apply online, we may need to be more alert to its role in regulating online activity and of the increased range of online activities regulated by contract. The point made in this brief essay is simple: the commercialisation of cyberspace correlates with an unprecedented proliferation of contractual relationships, some of which govern access to the Internet in the sense of connectivity (e.g. contracts with ISPs), while others regulate access to the content and services made available on websites (e.g. contracts with Amazon, Google etc). Both types of contracts can be regarded as a form of bottom-up regulation or private lawmaking. The latter term seems more apposite than "self-regulation." To explain: regulation can be imposed or self-adopted, top-down or bottom-up. [4] The latter implies a degree of voluntariness and self-determination; the former is associated with state authority and legislation. Bottom-up regulation can be synonymous with self-regulation or private lawmaking. Although "self-regulation" usually refers to rules developed by those participating in an activity, it often assumes the delegation of state authority.[5] Such delegation is, however, absent if bottom-up regulation takes the form of private agreement. It is also difficult to speak of *self*-regulation if the terms of such agreements are unilaterally imposed and if consent to them is largely fictional. There is no perfect term to describe the type of regulation encountered in commercial cyberspace. We can only observe that it takes the form of contracts governing a wide range of relationships, some of which may have no offline equivalent. If we recognise contract as a form of private lawmaking, we must examine its basic building block: consent.

---

[3] Manuel Castells, *The Rise of the Network Society* (Wiley & Sons, 2nd ed, 2010) 160.

[4] Julia Black, 'What is Regulatory Innovation?' in Julia Black, Martin Lodge and Mark Thatcher (eds), *Regulatory Innovation: A Comparative Analysis* (Edward Elgar, 2005) 11.

[5] Jeanne Pia Mifsud Bonnici, *Information Technology & Law Series: Self-Regulation in Cyberspace* (TCM Asser Press, 2008) vol 16, 6, 23.

Two problems arise. One concerns the form of consent, the other – the potential normative consequences of consent. To better understand these problems and to evaluate the very adequacy of contract-based private lawmaking we must revisit some early cyberspace scholarship.

I LESSONS FROM CYBERSPACE

In their famous 1996 article 'Law and Borders – The Rise of Law in Cyberspace,' Johnson and Post discussed the legitimacy of rule-setting "in" cyberspace and advocated a self-regulatory model as naturally deriving from the decentralised character of the Internet.[6] While many of their theories can be criticised as somewhat unrealistic, we must concede that some observations made by Johnson and Post retain their currency or, at the least, provide interesting points of departure for discussions concerning the regulation of online commerce. Three of them are pertinent for our purposes.

First, although it is frequently assumed that the said authors advocated that cyberspace remain lawless – a possible conflation with Barlow's declaration of *independence* of cyberspace[7] - Johnson and Post emphasised the need for *some* laws. They stated however, that such laws should be separate and different from traditional laws because only cyberspace-specific laws could accommodate the idiosyncrasies of the new environment. Existing laws were enacted with the physical world in mind and thus inherently unsuitable for cyberspace because they did not consider its characteristics. Recognising cyberspace as a separate regulatory sphere would simplify legal analysis by creating doctrines tailored to these characteristics.[8] The cyberspace-separatism advocated by Johnson & Post associated the lack of legitimacy of external regulators with their presumed lack of competence. After all, you cannot regulate something you don't understand.

Second, Johnson and Post asserted not only that every regulation had to allow for the characteristics of the place being regulated but also that these characteristics determined *who* should regulate - and cyberspace was inherently more amenable to bottom-up, self-regulatory efforts. Consequently, they emphasised the importance of private agreement in regulating cyberspace and promoted norms designed by "self-governing virtual communities" as reflecting the decentralised architecture of the Internet and the spirit of selfless

---

[6] David R Johnson and David Post, 'Law and Borders – The Raise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367, 1388.
[7] See John Perry Barlow, *A Declaration of the Independence of Cyberspace* (8 February 1996) Electronic Frontier Foundation <https://www.eff.org/cyberspace-independence>.
[8] Johnson and Post, above n 6, 1401.

co-operation.[9] Rules developed in virtual communities were better than state-imposed laws, because they were tailored *for and by* the participants themselves, reflecting their autonomy and competence. The legitimacy of the rules derived from the participation of those who were subject to those rules and who understood the environment they acted in.

Third, an important theme in Johnson & Post's article was the absence of physical borders. Borders were a precondition of enforceability within specific jurisdictions but also, on a broader level, served to delineate "spaces" and to establish which set of rules applied. In particular, borders had a signaling function. They provided notice that once the boundaries were crossed, the rules may change.[10] In cyberspace, borders would not serve to distinguish between jurisdictions but between commercial and non-commercial spaces or between different communities governed by discrete rules.[11] Borders also created context and, most importantly, shaped the expectations users had of their surroundings.

II 20 YEARS LATER

20 years later we can agree with most of the observations highlighted above, albeit with some qualifications. First, we can observe that the failure to understand the characteristics of the environment being regulated may have disastrous consequences. Examples abound. We can recall the overzealous top-down regulatory output of the late 90's and early 2000's, which is characterised by a general misunderstanding of most Internet-related technologies and business models.[12] Consequently, many of the Internet-specific top-down instruments enacted in that period were outdated on arrival, unnecessary or premature. Most of these instruments exhibit a certain "disconnect" between what they prescribe and what is technically possible or commercially necessary.[13] Second, as recommended *or anticipated* by Johnson & Post, the regulation of cyberspace has in fact evolved into a complex system of

---

[9] Lee Bygrave, 'Contract vs. Statute in Internet Governance' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edgar Elgar, 2013) 178.
[10] Johnson and Post, above n 6, 1370.
[11] Johnson and Post, above n 6, 1380.
[12] See generally: Chris Reed, 'How to make bad law: lessons from Cyberspace' (2010) 73 *Modern Law Review* 6; Susan P Crawford, 'The Internet and the Project of Communications Law' (2007) 55 *UCLA Law Review* 359, who observes that regulators seem to be "stumbling forward, tinkering blindly with the greatest value-creation system we have ever seen": at 381.
[13] Eliza Mik, 'E-commerce Regulation: Necessity, Futility, Disconnect' (Paper presented at First International Conference on Technologies and Law, Portugal, 8 November 2013) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2372559>.

predominantly private, bottom-up solutions.[14] There is no single cyberspace, but a myriad of self-regulated spaces where rules are imposed within localised areas of authority.[15] Some problems have, however, arisen that taint the optimistic roadmap painted by the authors. Johnson and Post did not anticipate the commercialisation of cyberspace and the difficulties of any meaningful *self*-regulation in a space governed by technological giants, such as Google or Amazon. Once businesses realised the potential of the Internet as a platform for content and service distribution, as a separate but equally viable sales and marketing channel - cyberspace became *commercial* cyberspace. And commercial cyberspace required more than community norms to recoup the investments in content and infrastructure. Once profits were to be made, cyberspace needed clear rules and the protection of the state in the form of enforceability. Enforceability, however, could only be granted to those relationships that carried the indicia of a contract.[16] Contract has thus naturally emerged as the dominant form of bottom-up regulation in commercial cyberspace. Although contract has always been regarded as a form of delegated legislative authority,[17] cyberspace has leveraged its role to an unprecedented level. Interestingly, despite the recognition that online commercial activity had to be anchored in a traditional legal framework, cyber-scholars have insisted that any external interference, be it legislative or judicial, be kept at a minimum as it could impede the development of "real legitimate internal governance."[18] Cyberspace should be regulated by means of contracts but such contracts should be left to market forces.[19] The assumption was (and maybe still is?) that market forces alone would produce contracts with the best possible terms. Users who disagreed with the norms of a given community could always exit and find a community with more suitable norms. This ease of exit would create a market for rules and naturally produce fairer terms. Of course, as it has

---

[14] Egbert Dommering, 'Regulating Technology: Code is not Law' in Egbert Dommering and Lodewijk F Asscher (eds), *Information Technology & Law Series: Coding Regulation, Essays on the Normative Role of Information Technology* (TCM Asser Press, 2006) vol 12, 10.

[15] Pierre Mounier, 'Internet Governance and the Question of Legitimacy' in Cécile Méadel, Eric Brousseau and Meryem Marzouki (eds), *Governance, Regulations and Powers on the Internet* (Cambridge University Press, 2012) 170.

[16] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a borderless world* (Oxford University Press, 2006) 138; Margaret Jane Radin and R. Polk Wagner, 'The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace' (1998) 73 *Chicago-Kent Law Review* 1295, 1296.

[17] Brian Coote, *Contract as Assumption, Essays on a Theme* (Hart Publishing, 2010) Ch 2 (Note: Chapter Two is a republication of Brian Coote, 'The Essence of Contract (Parts I and II)' (1988-89) 1 *Journal of Contract Law* 91; 183.

[18] David G Post, 'Governing Cyberspace' (2008) 24 *Santa Clara High Technology Law Journal* 883; Frank H Easterbrook, 'Cyberspace and the Law of the Horse' (1996) *University of Chicargo Legal Forum* 207, 215-216.

[19] Nicholas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) 25 *Berkeley Technology Law Journal* 1817, 1823.

turned out, most "online communities" are not communities but commercial relationships between those who provide online content or services (operators) and those who use such (users). These commercial relationships are governed by sets of standardised terms imposed by individual operators. It must be conceded that operators understand the characteristics of the environment better than external regulators. After all, they created (i.e. coded) the website or platform through which they conduct their business. The terms of these contracts are therefore perfectly tailored to the environment, the business model and, most importantly, the interests of the respective operators. As observed by Marsden, the "flood of private law" on the Internet reflects corporate interests not community values.[20] The problem does not, however, lie in the unilateral imposition of standard terms but in the fact that market forces have failed to produce the diversity of terms that were supposed to guarantee contractual fairness. Proponents of market determinism have ignored the difficulties of exit accompanying the network effects of the services provided by such companies as Facebook, Google, Amazon or eBay. They have also overlooked the fact that terms are routinely ignored. If, however, market participants do not review the terms – the market will not produce the best terms.[21]

I must pause to elaborate on the wide range of online relationships regulated by contract. Contracts govern not only traditional e-commerce transactions, such as purchases from Amazon or auctions on eBay but also the very access and use of many websites. We must consent to a set of terms either expressly, by e.g. establishing an account with a particular website, or impliedly, by continuing its use. We must do so even if we "only" want to read the news, "google something" or watch a cat video. As indicated, websites must often be regarded as access interfaces to online resources. As a consequence, contracts govern a broad spectrum of relationships, many of which do not appear *prima facie* commercial in nature. In many instances, online contracts are encountered in unfamiliar contexts. It may be unclear that the continued use of a website, or other online service, requires the formation of a contract. We must recall the third lesson from cyberspace: the importance of borders. While it is impossible to recreate *physical* borders online, there is a persistent trend in legal scholarship to demarcate various cyber-spaces: those that are open to everyone and those that require prior agreement. Madison speaks of the signaling function of borders in the context of notice of access restrictions to websites. As online experiences differ from offline experiences legal concepts "borrowed" from the physical world should be repackaged to match the online

[20] Christopher T Marsden, *Internet Co-Regulation* (Cambridge University Press, 2011) 6.
[21] Michael I Meyerson, 'The Efficient Consumer Form Contract: Law and Economics Meets the Real World' (1990) 24 *Georgia Law Review* 583, 601.

environment [22] Consequently, a party wishing to enforce any type of access conditions, such as those exemplified by website terms of use, should establish a "feature of the information environment that creates… a salient or visible boundary between open, public information and information subject to access constraints."[23] Translated into the present discussion, contract-based private lawmaking must allow for the characteristics of environment, particularly for the changed context in which online contracts are encountered. This dictates some form of enhanced notice, or "boundary," clearly signaling the very presence of terms. It is one thing, after all, not to expect contractual terms, it is yet another to deny their existence when they are conspicuously presented.

III THE PROBLEM WITH CONSENT

It is beyond doubt that the *legitimacy* of any rules appears questionable if they are unilaterally imposed. After all, the core justification for state non-interference is the "consent of the governed."[24] Private lawmaking, or "legitimate internal governance," can only be supported on the assumption that users consent to the contracts governing their relationships with online operators.[25] There are, however, multiple problems with contract-based private lawmaking most of which, quite surprisingly, derive from the very principles of contract law. The latter is inherently informal, permissive and content neutral. Formalities, such as writing or signatures, may be required by statute in the context of specific transactions, e.g. those relating to land. Otherwise, contractual intention – taking the form of acceptance, agreement or consent – can be manifested in any manner. Consequently, consent need not be express but can be inferred from any conduct, excluding silence but including the continued use of a website. Contract law is permissive in the sense that, assuming the absence of vitiating factors and illegality, the parties can agree on virtually anything. Substantive fairness is not required. Courts do not examine the adequacy of consideration or the equivalence of exchange. If one party agrees to relinquish her privacy in return for the "right" to watch cat videos – so be it. Contract law is content neutral in the sense that the same principles apply irrespective of the substance of the contractual provisions. One exception concerns enhanced notice requirements with regards to the incorporation of particularly onerous or unusual terms, popularly referred to as the "red hand rule."[26]

---

[22] Michael J Madison, 'Rights of Access and the Shape of the Internet' (2003) 44 *Boston College Law Review* 433, 489.
[23] Ibid 491.
[24] Johnson and Post, above n 6, 1370.
[25] Suzor, above n 19, 548.
[26] *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd* [1987] EWCA Civ 6.

Contrary to the foregoing, we intuitively expect consent to be express, deliberate and informed, not implied, accidental and uninformed. When faced with any form of contractual unfairness or when more significant rights are at stake, we recall that textbooks on contract law speak of the meeting of minds and of the voluntary assumption of obligations. We forget that theory differs from practice and that due to the principle of objectivity, the "meeting of minds" is not an actual requirement. We also tend to imply, somewhat irrationally, that "everything was perfect until commerce moved online." We forget that consent has been becoming increasingly less expressive and "easy to obtain" for more than a century. The "degradation of consent" accompanied the mass-market production of goods spawned by the industrial revolution. The latter has, in turn, lead to the standardisation of terms. Assumedly, the proliferation of standard terms was made possible by the simplicity and informality of contract formation. Moreover, contrary to popular assumptions, contractual terms need not be negotiated and can be unilaterally imposed. This has always been the case, long before the emergence of the Internet. Unsurprisingly, many academics question whether relationships based on standardised, unilaterally imposed terms can be referred to as contractual.[27] The accompanying problems have been described by Professor Radin in *Boilerplate*, a tirade on the aberrations of standard terms and the fictional character of consent. Radin recalls the traditional picture of contract as the time-honoured meeting of minds: two autonomous wills coming together to express their autonomy. She then describes the decay of consent, the progressive shift from voluntary willingness to fictional assent and, ultimately, to a "mere efficient rearrangement of entitlements without any consent or assent."[28] In her words:

> Consent seems obviously fictional in a great many transactions, however, and that is one reason I say that consent is vestigial. Consent is fictional when the terms are filed somewhere we cannot access, as in airline tariffs. Consent is fictional when almost all of us click on-screen boxes affirming that we have read and understood things we have not read and would not understand if we did. Consent is fictional on websites whose terms of service state that just by browsing the site, whether or

[27] See: Randy E Barnett, 'Consenting to Form Contracts' (2002) 71 *Fordham Law Review* 627, 627 (who observes the dissonance between contract theory and practice on the subject of form contracts); Omri Ben-Shahar, 'Foreword to Boilerplate: Foundation of Market Contracts Symposium' (2006) 104 *Michigan Law Review* 821, 826 ("On a theoretical level, boilerplate is shown to be a legal phenomenon different from contract. Is it a statute? Is it property? Is it a product?").

[28] Margaret Jane Radin, 'Boilerplate Today: The Rise Of Modularity And The Waning Of Consent' (2006) 104 *Michigan Law Review* 1223.

> not one ever clicks on the terms, one has agreed to whatever the terms say, now or as they may be changed in the future. Consent is fictional when the contract ends, as one I saw recently did, with "By reading the above you have agreed to it."[29]

The degradation of consent, next to the imposition of one-sided standardised terms, can be regarded as the main weakness of contract-based private lawmaking. We must, however, re-emphasise that this weakness is not attributable to the Internet or to the commercialisation of cyberspace. The degradation of consent is best explained with the concept of "shifting baseline syndrome." Dan Pauly presents the term in the context of the ecology of fisheries: each generation of fisheries scientists accept as a baseline the stock size that occurred at the beginning of their careers and uses it to evaluate changes. Years later, when the next generation starts its career, the stocks have declined further, but it is these stocks at that time that serve as a new baseline.[30] The result is a gradual shift of the baseline, a slow barely perceptible accumulation of negative changes. At some stage, someone asks: *where are all the fish gone?* But at that stage - it is probably too late. In the context of contract law we might ask *why is consent so easy to obtain?* Or: how can it be implied from so many behaviours that do not carry the same gravity or solemnity as signatures or handshakes? How can *billions* of contractual relationships be created with something as informal as a click? Clicks, or other forms of interacting with artificial interfaces, are always used as illustrations of a problem that is, strictly speaking, unrelated to the web or the Internet. Before blaming the Internet we must ask: what should be regarded as the baseline for evaluating contractual consent? Is it the informed and deliberate consent encountered in face-to-face negotiations between peers or the semi-accidental cursory consent encountered in mass-market, standardised transactions that characterise *everyday* commerce? Should we compare consent in online contracts to the former or the latter? It becomes apparent that the degradation of consent cannot be attributed to the web or to the Internet. The latter may have *slightly* contributed to the shift in the baseline in the sense that it simplified the contracting process even further. After all, web-based interactions are streamlined to the point of making consent so simple as to render it virtually imperceptible and thus meaningless. It may, however, also be claimed that online commerce did not contribute but simply took advantage of a pre-existing problem. Operators exploit a *status quo* that is the result of a long-term trend. The baseline shifted long before the Internet became mainstream. If we regard everyday commercial practice, including consumer

---

[29] Ibid 1223, 1231.

[30] Dan Pauly, 'Anecdotes and the Shifting Baseline Syndrome of Fisheries' (1995) 10 *Trends in Ecology and Evolution* 430.

transactions, as the baseline for contractual consent it becomes apparent that online transactions do not significantly depart from that baseline. The progressive degradation of consent can be blamed on prior generations of commercially minded judges that resigned themselves to the demands of the market – not on the Internet.

Despite its degradation, consent has become more significant in terms of its potential normative consequences. Users impliedly (or *inadvertently*?) "consent" to increasingly important matters, such as the alienation of rights or the assumption of obligations that may prove detrimental to their long-term interests. For example, millions of users "consent" to what is best described as pervasive commercial surveillance on a daily basis. To explain: the web consists of a complex ecosystem of vendors, advertisers, content and service providers, to name a few. The predominant business models rely on advertising. Money is made (directly or indirectly) not only when consumers purchase books on Amazon or subscriptions to Netflix, but also when they click on advertisements or otherwise interact with content. [31] Despite popular references to "free" online services, the online environment abounds in transactions conditioning access to online resources on "payment" with personal information. In the latter instance, the transactional context may be barely perceptible because there is no price indication and no provision of payment data. Consequently, users who want to read the news or listen to music consent to the operators' collecting, analysing and subsequently utilising their personal information. Aside from the simplicity of implied consent, another problem concerns the fact that users need not understand what they are consenting to. Contractual consent need not be informed. It is therefore irrelevant that the terms (provided via hyperlink on the bottom of websites or "popping-up" during account creation) are never read.[32] It suffices that the user has the opportunity to review them. This is where the differences between the online and the offline environments become apparent. Unlike in traditional offline transactions, users have a realistic chance to read online terms without time constraints and pressures from over-zealous sales assistants. [33] At the same time, however, they do not expect terms and often do not understand the relevance of the "terms of use" hyperlink at the bottom of the webpage. More importantly, websites are meticulously designed to encourage or

[31] For a succinct explanation see Richard Warner and Robert H Sloan, 'Behavioral Advertising: From One-Sided Chicken to Informational Norms' (2012) 15 *Vanderbilt Journal Entertainment & Technology Law* 49, 57-60.
[32] David R Trossen, 'Florencia Marotta-Wurgler and Yannis Bakos 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts' (2014) 43 *Journal of Legal Studies* 1.
[33] Robert A Hillman, 'Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?' (2006) 104 *Michigan Law Review* 837.

discourage certain actions, *including* the reading of terms. [34] We must not forget that operators not only impose the terms but also control the entire transacting environment, which results in an unprecedented degree of "technological management" of users, including novel ways of manipulating their behavior.[35]

IV FINAL OBSERVATIONS

An interesting picture emerges. On one hand, top-down regulators rarely have the expertise to efficiently regulate the online environment. In some instances, it could even be questioned whether such top-down regulation is necessary to begin with. The dangers of bad regulation are exemplified by the failed EU directives aimed at 'facilitating' e-commerce and digital signatures. On the other, bottom-up regulations in the form of private agreements carry their own disadvantages, predominantly related to the permissive and informal character of contract law and the increasingly fictional character of consent. If consent can be obtained too easily while, at the same time, it carries significant normative consequences, some external assistance may be necessary. An indiscriminate reliance on market forces overlooks the necessity to control private power – in our case, that of Internet giants like Google or Amazon. As early as 1944, Kessler emphasised that unlimited freedom of contract enables enterprisers to legislate by contract, often "in a substantially authoritarian manner without using the appearance of authoritarian forms."[36] Similarly, Coote admitted that unless the parties are of equal bargaining power or if the stronger party is prepared to exercise self-restraint, freedom of contract could be an instrument of oppression. [37] More recently, Suzor suggests that we should see many online contracts as "mini-constitutions" and recognise their role in unilaterally shaping billions of relationships and their potential for subverting values. [38] The fact that contract has become a tool of shaping rights in billions of relationships does not, however, change the principles of contract law. At the same time, we may require a more discerning approach in how these principles are applied. The boundaries of contract-based private lawmaking must be influenced not only by the strict application of contractual principles but also by certain substantive values. It is one thing to say that contract law continues to apply online, it is yet another to realise how contract is used in the online economy. It could be argued that if contracts effectively

---

[34] Ryan Calo, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995, 1034.
[35] Roger Brownsword, 'The Shaping Of Our On-Line Worlds: Getting The Regulatory Environment Right' (2012) 20 *International Journal of Law and Technology* 249, 253.
[36] Friedrich Kessler, 'Contracts of Adhesion – Some Thoughts about Freedom of Contract' (1943) 43 *Columbia Law Review* 629, 640.
[37] Coote, above n 17, 33.
[38] Nicols Suzor, 'Order Supported by Law: The Enforcement of Rules in Online Communities' (2012) 63 *Mercer Law Review* 523, 523.

become constitutions, then both the substance of these contracts and the process of their formation should be influenced by principles of public governance.[39] The "easiest" solution seems to be the creation of rules dictating that consent that produces normative effects, such as the assumption of obligations or the relinquishment of important rights, should be express or more expressive. This "solution" creates a cascade of difficult questions: *who* should introduce such rule and *how*? Should such "enhanced consent" be imposed by judges or by the legislature? What form should it take? Would it resemble cookie notification bars in the EU or the "click-wrap" agreements encountered in the US? In what circumstances would it be necessary? How would such requirement affect legal certainty? It must not be forgotten that contract law itself does not recognise the concept of "enhanced consent" – any external additions to its principles should be approached with caution. At the same time, leaving aside doctrinal purity, it cannot be doubted that some form of 'adjustment' is indispensable. The present state of affairs can be regarded as a mockery of both contract and of self-regulation.

[39] Ibid; Anupam Chander, 'Facebookistan' (2012) 90 *North Carolina Law Review* 1808.

Defining Cybercrime Based on Roles of Data Processing Systems

Xingan Li*

ABSTRACT

The purpose of this article is to perform theoretical study of cybercrime through defining the phenomenon based on evaluation of earlier investigation. The article reviews the previous notions of computer crime and cybercrime and explores into deficiencies of previous definitions. The article also gives explanation to the socio-technical implications of employing the label "cyber". The article suggests a comprehensive definition of cybercrime as any type or any form of traditional or untraditional crime involving data processing systems in use as mass media, operating mechanism, place of occurrence, transfer channel, targeted object, and multiple-purpose instrument, or used in the preparation for other crimes and theoretically expands the roles of data processing systems in cybercrime.

Keywords: Cybercrime; Cyberspace; Definition; Role of information; Informatics

I INTRODUCTION

More than ever before, users of cyberspace are confronted with growing new visions in the 21st century, wrestling with cyber security and cybercrime.[1] Besides the data processing system and the Internet, presently, cloud computing, social networking services and blockchain technology are three of the most recent attractive examples. Although pervasive use of data processing systems is accompanied by an extensive scope of social problems, and the countermeasures demand mobilising a wide array of legal remedies, this article will principally be concentrated on criminal phenomena exploiting data processing systems. Consequently, the focal mission facing us is to determine the scope of the topic, through defining the subject-matter "cybercrime".[2]

---

* Associate Professor, School of Governance, Law and Society, Tallinn University.

[1] Xingan Li, *Cybersecurity and Cybercrime in the 21st Century* (Informyth, 2016).

[2] See also the author's previous research, Xingan Li, *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society* (University of Turku, 2008).

Different definitions of cybercrime have surfaced over the years as users and abusers of data processing systems expanded into novel locales. There is neither a unified definition, nor a universally established approach to classification. The definition and classification methods are so diversified that it is impractical to draw the scenario of cybercrime by adopting a particular benchmark.[3] The current rampancy of cybercrime can partially be understood as the result of weak legal prevention.

The purpose of this article is to perform a theoretical analysis of cybercrime through defining cybercrime based on examination of previous research. Following this introduction, the article goes on to investigate previous notions on computer crime, giving concise assessment of the deficiencies of conventional definitions. The article will also interpret the techno-legal implication of the label "cyber". In the latter part, this article will advocate the use of a unified broad definition of cybercrime, in order to accomplish a consensus as great as possible, reform both substantive and procedural criminal law and provide effective protection for the information society.

II EVOLUTION OF CONCEPTS OF COMPUTER CRIME

Prior to the 1990s, computer crimes were in general understood as offences relating to computers, but there was less connection with networks, which were also exploited by the perpetrators of earlier computer crimes. Amongst scholars, the arguments pertaining to the association between computers and crime were diverse. Even in the present day, there is no noticeable distinction between a computer crime and a traditional crime that has a few factors relating to data processing systems. The situation in the pre-Internet era should without difficulty be comprehended from the current standpoint. Nonetheless, the most remarkable disagreement at that time revolved around the question of whether there was a distinctive criminal phenomenon of computer crime. Roughly speaking, three different perspectives existed.

One perspective negated the existence of computer crime. For instance, Johnson insisted that there was no dissimilarity between a wrongdoing involving a computer and a wrongdoing involving no computer.[4] Gotternbarn also argued that a particular group of computer crime was redundant.[5] Those who negated computer crime as a special type of crime only classified computer crimes into traditional crimes. Because slaughter with a stick, a

---

[3] Martin Wasik, *Crime and the Computer* (Clarendon Press, 1991) 1.
[4] Deborah G Johnson, *Computer Ethics* (Prentice Hall, 1985).
[5] Donald Gotterbarn, 'Computer Ethics: Responsibility Regained' (1990) 71(3) *National Forum: The Phi Kappa Phi Journal* 26. Reprinted in Deborah G Johnson and Helen Nissenbaum (eds), *Computers, Ethics and Social Values* (Prentice Hall, 1995) 18.

stone, a knife, a gun, or a bomb, was simply a slaughter, logically stealing with a bag, a car, or a computer remained just an act of stealing. The "new" types of crimes or new forms of existing crimes could, from this perspective, be covered by traditional criminal law. There were, for that reason, no new amendments required to existing law. The mere task was to penalise these crimes according to the old law.

Another perspective, considered to be a pan-computer crime outlook,[6] alleged that the computer could be used to commit all kinds of offences. According to Sterling, Donn B. Parker argued that "…all business crime will be computer crime, because businesses will do everything through computers. 'Computer crime' as a category will vanish."[7] Li suggested that computer crime was neither a single offence, nor a category of offences; only because the offences essentially involved data processing systems, they were called computer crimes. In fact, this term can both refer to one single computer crime and to one category,[8] thus the scope is broad.

Li also endeavoured to apply conventional criminal law stipulations to a variety of computer crimes, in examining the likelihood of using the 1979 Penal Law of China to impose a penalty on all offences involving computers against state security, person, property, and the social order.[9] Such a proposal was also a commonly acknowledged initiative about dealing with computer crime in many countries then. The proof was that many countries punished the earliest computer crimes prior to implementing their first computer crime laws. At least in countries where a broad legal interpretation and judicial legislation were practised, unpunished computer crime cases due to lack of applicable law were rare. But the *analogous application of law* by extending the scope of existing law to impose punishment on activities that were not prescribed by law when they were committed is excluded by the principle of legality. The *broad interpretation of law* did not necessarily, nevertheless, contravene the principle of legality, even though the interpretation incorporated new terms, for example the computer, the Internet and data processing systems, into law where these terms were on one occasion missing. The importance of this perspective was to make the potential of conventional

---

[6] Susan H Nycum, 'Testimony on Computer Security before the U. S. Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs' (1984) 13(4) & 14(1-3) *Computers and Society*.

[7] Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (Project Gutenberg EBook, 1994) <http://www.gutenberg.org/dirs/etext94/hack12.txt>.

[8] Xingan Li, *Jisuanji Fanzui Ruogan Wenti zhi Yanjiu* (A Study on Several Issues of Computer Crime) (Master of Laws Thesis, China University of Political Science and Law, 1993).

[9] Xingan Li, 'Lun Jusuanji Fanzui Xingfa Shiyong Wenti (Concerning the Application of Penal Law to Computer Crime)' [1992] (2) *Graduate Law Review, China University of Political Science and Law*.

criminal law as grand as possible. Where there is no law prepared to fight computer crime, this perspective supplies a theoretical foundation for the application of existing laws to both safeguarding society and preserving legality.

Actually, as Bequai noted that, "the majority of our local jurisdictions rely on traditional concepts to deal with this new and growing area of crime",[10] including laws dealing with crimes involving habitation and occupation, covering arson and burglary, and laws dealing with offences involving property, covering larceny, embezzlement, extortion, malicious mischief and forgery.[11] Recent efforts for utilising the functions of existing criminal law have also been made by Brenner.[12]

Finally, the third perspective acknowledged the existence of computer crime on the one hand, but limited the scope of offences on the other. Unquestionably, this has been the theory most broadly accepted. According to this theory, different technical terms have been used to indicate the phenomenon, different definitions have been given to illustrate the topic, and different theoretical achievements have been acquired to address the legal framework. On the other hand, there has not been a unified technical term, a unified definition,[13] or a unified theoretical structure of an internationally accepted classification. Numerous technical terms have been used interchangeably.[14] Different countries and individuals have proposed many definitions. Additionally, people from different academic fields have also initiated many theoretical agendas over the years. At the present time, when we talk about computer crime, or cybercrime, a straight reflection is the postulation that computers or networks are involved in this crime.

The phenomenon of computer crime has been defined in a diverse spectrum of senses, from exceedingly constricted ones to exceedingly extensive ones.

---

[10] August Bequai, *Computer Crime* (Lexington Books, 1978).
[11] Ibid.
[12] Susan W Brenner, Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law (2001) 8(2) *eLaw Journal: Murdoch University Electronic Journal of Law* 1 <http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html>.
[13] United Nations Crime and Justice Information Network, 'International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-Related Crime' (1999) 43-44 *International Review of Criminal Policy*.
[14] See Commission of the European Communities, 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime' (Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM/2000/890 final) 12. Even the UN uses the terms computer crime and computer-related crime interchangeably. See also ibid [21].

The definition in the most constricted sense limits computer crime to "one that can be carried out only through the use of computer technology".[15] This definition leave out crimes that can be committed merely through other means than by using computer technology and that can be committed in both ways. In a broader manner, computer crime is defined as crime by computer. This definition rules out crimes targeting a computer.

In a wider sense, a definition includes both crimes by computer and against the computer.[16] Crimes against the computer can be committed by both conventional and nonconventional methods. There were abundant cases in which computers were damaged not by today's technological methods, such as viruses, illegal access etc., but were committed in traditionally violent ways, including arson, bombing, and shooting. The development of cybercriminal phenomena demonstrates that there is an indistinguishable boundary between offences by computer and offences against the computer.

The broadest definition was advised by Parker, who divided computer crimes into computer abuse, computer crime and computer-related crime.[17] Observably, the computer crime conception at the second level was included in the first level. The computer crime conception at the first level was exceptionally broad. Indeed, Parker and Nycum defined computer crime "as any illegal act where a specific knowledge of computer technology is essential for its perpetration, investigation, or prosecution," saying subsequently that computer crime was not regarded as a distinct type of crime different from other crimes, and that approximately all sorts of crimes could be committed through the utilisation or involvement of computers.[18] Such a definition has be accepted and developed by numerous following studies, for example, Pihlajamäki defined cybercrime ("information technology crime" in his original term) as a crime in which the data processing system is the target or tool, while special knowledge of information technology is a necessary factor

---

[15] Herman T Tavani, 'Defining the Boundaries of Computer Crime: Piracy, Break-ins, and Sabotage in Cyberspace' (2000) 30(4) *Computers and* Society 3.

[16] See, for example, McConnell International, *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information* (2000) <http://www.witsa.org/papers/McConnell-cybercrime.pdf>. See also Terrence Berg, 'WWW.Wildwest.gov: The Impact of the Internet on State Power to Enforce the Law' (2000) 2000(4) *Brigham Young University Law Review* 1305; Marc D Goodman, 'Why the Police Don't Care About Computer Crime' (1997) 10(3) *Harvard Journal of Law and Technology* 465.

[17] Donn B Parker, 'Computer Abuse Research Update' (1980) 2(2) *Computer Law Journal* 329, cited in Artur Solarz *Computer Technology and Computer Crime* (US Department of Justice, 1981).

[18] Donn B Parker and Susan H Nycum, 'Computer Crime' (1984) 27(4) *Communication of the ACM* 313.

in the process of commission and prosecution.[19]

Due to pervasion of computer networks, the model of a computer crime becomes more pertinent with the appearance of the Internet. Cybercrime is loosely defined as a crime committed by means of a computer or the Internet.[20] The Council of Europe Convention on Cybercrime 2001 made the term "cybercrime" ubiquitous. Articles 2-10 of the Convention on Cybercrime also adopted a broad conception in criminalising cybercrime, stipulating the offences against security, computer-related offences, and content-related offences. Although the Convention adopted a broad conception, the detailed offences under these titles were limited. The high level of consensus concerning conception, and the low level of consensus concerning the categories is a factor that makes it unenthusiastic for more countries to consider access to the agreement.

III NON-TECHNOLOGICAL MISUNDERSTANDINGS OF CYBERCRIME

The various previous ways of understanding cybercrime have been ambiguous and perplexing by providing imprecise information. The following deficiencies have been very frequent in both academic and non-academic writings.

The first misunderstanding happened against a historical background. While people have regarded the predecessors of cybercriminals as the hackers of three or four decades ago, a general view has been to make the term "hacking" bear the meanings of today's "cybercrime". This misunderstanding buried the computer explorers collectively under the shell of deviance.

The second misunderstanding, the equation "cybercrime = cyber terrorism" has already been broadly accepted with the help of mass media. As yet, although there have been many concerns about the use of data processing systems in the preparation of real terrorist attacks, and the situation may be growing worse,[21] cyber terrorism is only a political possibility. By claiming all

---

[19] Antti Pihlajamäki, *Tietojenkäsittelyrauhan rikosoikeudellinen suoja: datarikoksia koskeva sääntely Suomen rikoslaissa* (The Protection of Data Processing under Criminal Law: Provisions on Data Crimes in the Finnish Criminal Code) (Suomalainen lakimiesyhdistys, 2004) 286.

[20] David Levinson (ed), *Encyclopedia of Crime and Punishment* (Sage Publications, 2002) 455.

[21] Many prosecuted cases involved features that were possibly to be used in terrorist attacks deposited in data processing systemdata processing systems, for example, *R v Boutrab* [2005] NICC 36 (24 November 2005), in which the accused downloaded from a library computer and deposited in floppy discs the files, the contents of which contained information about the making and use of explosives for attacks on aircraft and the manufacture of silencers for firearms.

cybercrime as cyber terrorism, the future of the communities in the information society is obscure.

The third misunderstanding is politicisation of the conception in a broader sense. To view cybercrime as cyber terrorism is one part of the picture. This broad misunderstanding was created by the acclamation of data processing systems as a national critical infrastructure, the maintenance and protection of which purportedly making state intervention or political intervention necessary. The politicization of data processing systems results in the politicisation of activities against this system, the cybercrime.

The fourth misleading understanding is, strangely, to moralise the cybercrime by exploiting the term "hacking". The moralisation has two aspects: one regards cybercrime as being moral, not immoral and thus not illegal; the other regards cybercrime as a moral issue, not a legal issue, and thus law has no business here. The natural effect is that cybercrime should not be regulated by law.

The last category of misleading definitions has the tendency of mystification. The representative notion is that cybercrime is high-tech crime and does not seem to be committable by common users in daily life. Actually, when technology is used in routine life, high technology gradually becomes "low" technology. When high tech crime exists in daily life, it becomes low-tech crime.

IV CLASSIFICATION OF NOMENCLATURE

No unified term for cybercriminal phenomena has been universally accepted, even though some terms including "computer crime" and "cybercrime" are relatively popular. Generally, seven groups of terms have been in use. Among these groups, many different words and phrases have been adopted or created. Owing to the changing ways in which the cybercriminals commit crimes, the ways in which people designate these crimes are changing as well. In order to elucidate how people view cybercrime from different standpoints, this section examines some groups of synonymous terminologies of "cybercrime".

The first group emphasises the computer as a unique target or tool of crime. The term "computer crime" has been broadly used in academic writings as well as in laws and regulations particularly before the 1990s when the Internet was not opened to commercial use. This term represents a group of similar

terms, including computer crime,[22] crime by computer,[23] computer-related crime,[24] computer-facilitated crime,[25] computer misuse,[26] computer abuse,[27] computer mischief,[28] computer break-in,[29] computer sabotage,[30] computer espionage,[31] computer manipulation,[32] etc. "Comcrime" was used in the title of Sieber,[33] though the term was not used in the main body of the text.

The second group is accompanied with a crime particularly facilitated by computer networks. The origin of the term "cybercrime" cannot be identified, but there is no doubt that it became prevalent with the legislating process of the European Convention on Cybercrime. The prefix "cyber" simply means computer, but people tend to use it in terms of networked computers. Generally, people expect to make a distinction between the criminal phenomena in the network age from that before the 1990s when isolated computers played a more significant role. Smith, Grabosky and Urbas have argued that "cyber" used as an adjective does not equal to "cyber-" used as a prefix.[34] That is to say, "cyber crime" is not "cybercrime". They have used the

---

[22] Computer crime is the most frequently used term in denoting the phenomenon. For example, there is an institution named the "Computer Crime Research Centre". See the institution's Web site, at <http://www.crime-research.org/>.

[23] Donn B. Parker, *Crime by Computer* (Charles Scribner's Sons, 1976).

[24] Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME–Study* (Report prepared for the European Commission, 1998) <http://www.oas.org/juridico/english/COMCRIME%20Study.pdf>; Peter Stephenson, *Investigating Computer-Related Crime* (CRC Press LLC, 2000).

[25] See Computer Crime and Intellectual Property Section (CCIPS), *Prosecuting Crimes Facilitated by Computers and by the Internet* (15 March 2007) <http://www.usdoj.gov/criminal/cybercrime/crimes.html>.

[26] For example, the usage of this term in the United Kingdom *Computer Misuse Act 1990* (UK) c 18.

[27] For example, the usage of this term in the United States *Computer Fraud and Abuse Act*, 18 USC § 1030.

[28] See, for example, Curt Woodward, *Washington Quarter Voting Hijacked by Computer Mischief* (10 April 2006) Associated Press <http://seattlepi.nwsource.com/local/6420AP_WA_State_Quarter.html>. See also unofficial English translation (by the Finnish Ministry of Justice) of the Penal Code of Finland, Chapter 34, Section 9a (578/1995) .

[29] See also unofficial English translation (by the Finnish Ministry of Justice) of the Penal Code of Finland, Chapter 34, Section 8 (578/1995).

[30] Ulrich Sieber, 'Computer Crime and Criminal Information Law – New Trends in the International Risk and Information Society - Statement for the Hearing on Security in Cyberspace of the United States Senate' (Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 1996).

[31] Defence Investigation Service, 'Computer Espionage' (1996) 288 *The American Report* <http://www.kimsoft.com/korea/edispy.htm>; Joel McNamara, *Secrets of Computer Espionage: Tactics and Countermeasures* (John Wiley and Sons, 2003).

[32] Sieber, above n 30.

[33] Sieber, above n 24.

[34] Russell G Smith, Peter Grabosky, and Gregor Urbas, *Cyber Criminals on Trial* (Cambridge University Press, 2004).

term "cyber crime" "to describe a range of criminal offences, only some of which specifically relate to computers and the telecommunications infrastructure that supports their use." [35] They have viewed "cybercrime" as "a singular concept of crime that can encompass new criminal offences perpetrated in new ways," and "cyber crime" as "a descriptive term for a type of crime involving conventional crimes perpetrated using new technologies." [36] Most authors are using these two terms interchangeably. Besides the terms cybercrime, or cyber crime, people also use net crime,[37] Internet crime,[38] crime on the Internet,[39] Internet-related crime,[40] network crime,[41] etc. In Finland, cybercrime is sometimes translated as "tietoverkkorikos" (information network crime), with the same meaning as "tietotekniikkarikos" (information technique crime), referring to both offences targeting information processing systems and offences committed with the assistance of information processing systems.[42] According to Darlington, crimes on the Internet include "hacking, viruses, pirating, illegal trading, fraud, scams, money laundering, prescription drugs, defamatory libel, cyber stalking, cyber terrorism."[43] According to CCIPS, Internet-related crimes include "computer intrusion, password trafficking, copyright piracy, theft of trade secrets, trademark counterfeiting, counterfeiting of currency, child pornography or exploitation, child exploitation and Internet fraud matters that have a mail nexus, Internet fraud and spam, Internet harassment, Internet bomb threats, trafficking in explosive or incendiary devices or firearms over the Internet."[44]

The third group views the Internet as only a part of the whole telecommunications systems.[45] Electronic crime (e-crime) emphasises the

---

[35] Ibid 5.

[36] Ibid 6.

[37] For example, the term net crime was used in news report, E Luening, *European Council Moves Net Crime Treaty Forward* (3 January 2002) CNET News <http://www.cnet.com/au/news/ european-council-moves-net-crime-treaty-forward/>.

[38] Max Taylor, and Ethel Quayle, *Child Pornography: An Internet Crime* (Brunner-Routledge, 2003).

[39] For example, Roger Darlington, *Crime on the Internet* (1 July 2016) <http://www.roger darlington.co.uk/crimeonthenet.html>.

[40] For example, Computer Crime and Intellectual Property Section (CCIPS), *How to Report Internet-Related Crime* (2015) <https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime>.

[41] In Chinese, the counterpart of the term cybercrime is simply "wangluo fanzui" (network crime).

[42] Governmental Proposal HE 153/2006 of Finland concerning Approval of Council of Europe Convention on Cybercrime (hereafter HE 153/2006), General Justifications, 1. Introduction.

[43] Darlington, above n 39.

[44] CCIPS, *Computer Intrusion Cases* (2006) <http://www.usdoj.gov/criminal/cybercrime/ cccases.html>.

[45] For example Amy Tennyenhuis, and Rodger Jamieson, 'Multidisciplinary E-Forensics Methodology Development to Assist in the Investigation of E-Crime' in Kim V Anderson, Steve Elliot, Paula M C Swatman, Eileen Trauth and Niels Bjorn-Anderson (eds), *Seeking Success*

characteristic of the criminal phenomena relating to (micro) electronics rather than to computers or computer networks. With this term, people usually indicate the same phenomenon as cybercrime, but others also extend it to cover crimes relating to the telecommunications systems, in which the Internet is only a part.

The fourth group locates the space, the community, or the environment created by the Internet where a crime is committed. The word "virtual" has a deep and different meaning in the term "virtual reality",[46] but "virtual crime" is in fact the substitute of cybercrime in the sense that the crime is committed in the network environment. A purely virtual crime has not been criminalised.[47] When used as synonym for cybercrime, the focus of the term "virtual crime" is put into the specific spatiotemporal context created by the Internet and interpersonal communication via the Internet.

The fifth group differentiates the data, information or privacy as the primary factor in a crime. In fact, cybercrime is crime related to information or data processing systems (not limited to computers and computer networks). Future terminology should therefore incorporate information or data processing systems into the name of such a crime.

The sixth group characterises the uniqueness of the processing of "digital" information in cybercrime.[48] "Digital" means "using a system in which information is recorded or sent out electronically in the form of numbers, usually ones and zeros."[49] Digits are neither the system through which the crime is committed, nor the technology by which the crime is committed. Rather, they are the form in which information is processed through the system. A crime can hardly be "digital" because the committing process of a crime differs from the processing form of information.

The seventh group reveals the role of ICT as high technology. A crime involving ICT is named high technology crime,[50] high-tech crime,[51] hi-tech

---

in E-Business: A Multidisciplinary Approach (Kluwer Academic Publishers, 2003) 187.

[46] See Della Summers, *Longman Dictionary of Contemporary English* (Pearson Education Limited, 4th ed, 2003) 1841.

[47] Such as the case of "a rape in cyberspace" described in Julian Dibbell, 'A Rape in Cyberspace' (1993) 38(51) *Village Voice* 36. The article described a "cyberrape" performed by a Mr. Bungle in a multi-user dungeon (MUD), called LambdaMoo, and the repercussions of his act.

[48] Peter Lilley, *Hacked, Attacked, and Abused: Digital Crime Exposed* (Kogan Page Limited, 2002).

[49] Summers, above n 47, 436.

[50] Gerald Kovacich, and William C Boni, *High Technology Crime Investigator's Handbook: Working in the Global Information Environment* (Butterworth-Heinemann, 1999); the International High Technology Crime Investigation Association (HTCIA)," is designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge

crime,[52] or information technique crime.[53] In fact, the term "high technology" is only used to indicate modern high technology, excluding the ancient ones. In the viewpoint of the tenth century, papermaking may be a high technology. In the viewpoint of fourteenth century, movable type printing techniques may be another high technology. They can both be regarded as technology relating to information processing. This indicates that the term high technology is inappropriate for designating a crime. On the other hand, most computer-related crimes have in fact only used "low tech" as Molnar found in his study.[54] As a result, there has been a misunderstanding in giving the impression that each and every kind of computer crime is sophisticated and not committed by ordinary persons. [55]

V TECHNO-LEGAL IMPLICATIONS OF THE LABEL "CYBER"

As noted, the prevalence of the prefix "cyber" readily becomes a substitute for the terms computer and computer network. Anything can be "cyber" if it is related to the computer and the computer network. One of crime's labels currently in use is "cyber." The following is only an effort to explore the subtext to which the prefix "cyber" can refer.

1. Implying deviant behaviours dependent on data processing systems. Violent crime is a label for deviant behaviours involving the use of human force. Intelligent crime is a label for deviant behaviours involving the use of wisdom. White-collar crime is a label for deviant behaviours by the perpetrator's occupation. Similarly, cybercrime labels deviant behaviours that depend on data processing systems, without which the offences are impossible to commit,

---

about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.": HTCIA, *About Us* (2016) <http://www.htcia.org/aboutus.shtml>.

[51] For example, "Australian High Tech Crime Centre", "employs representatives from all Australian State and Territory police forces in both its staff and its Board of Management. This creates an environment of cooperation and national consistency to referrals, training, education, intelligence, policy and investigations." See Australian High Tech Crime Centre, *Home* <http://www.ahtcc.gov.au/>.

[52] For example, an institution named "The National Hi Tech Crime Unit", which is part of the Serious Organised Crime Agency. See <http://www.nhtcu.org/>.

[53] For example, in Finnish, the literal meaning of the term "tietotekniikkarikos" is information technique crime. The term is used interchangeably with "tietoverkkorikos" (information network crime) (HE 153/2006, General Justifications, 1. Introduction). The general understanding of cybercrime is that it happens in the environment of information processing systems and with an expertise on the operation of such systems (ibid).

[54] Jack Molnar, 'Putting Computer-related Crime in Perspective' (1987) 6(4) *Journal of Policy Analysis and Management* 714.

[55] Ibid.

or by which the offences may be committed more efficiently.[56] The more the people are heavily dependent on data processing systems, the more the offences that cannot be committed without such systems are committed; the more efficiently the offences with such a system can be committed, the more frequently they occur. The prefix "cyber" is meant to characterise the dependence of new types or new categories of offences on data processing systems which label this society.

2. Sketching the semi-virtual and semi-real crime scene. Many people are talking about a different space as virtual. Actually, due to technological limits, perfect virtual space has not been realised. The current cyberspace is a semi-virtual and semi-real space. Thus, pure virtual interaction is neither possible nor has its meaning. The information age is a term symbolising a developing stage of virtual space, a partially virtual and partially real environment. Naturally, cybercrime only involves a semi-virtual and semi-real crime scene. It is true that the supposed neural computer may construct a pure virtual atmosphere and facilitate a pure virtual crime. However, the virtual crime scene cannot appear before a robot driven by a neural computer is created.

3. Demonstrating human-machine criminal interactions. Human-machine interaction represents just a piece of social interactions. The results of human-machine interaction can be human-machine-human or human-machine-machine interactions. The process can be unlimitedly expanded. Furthermore, the participants in the interaction can be multiple humans and multiple machines, that is, in networked systems. This shows the complicacy of online activities including cybercrime. In fact, the human-machine interaction has a deep impact on the criminalisation of deviant behaviours relating to data processing systems. For example, in the Governmental Proposal HE 153/2006 (Finland), the spreading of computer virus has been noted as likely to be realised through delivering it to other persons, or through spreading it in the machines.[57]

4. Illustrating an extension of the criminal territory. The traditional crime happens in the visible sphere and is mostly territory-dependent. In the information age, the territorial extension of crime has dual meanings. On the one hand, the criminal phenomenon extends from the visible sphere to the invisible sphere. Cybercrime generally crosses both visible and invisible spheres simultaneously. The process and results of cybercrime are both

[56] See Bequai, above n 10, 1. Considering that the concept of white-collar crime is becoming vague in the information age, this study generally does not classify cybercrime into the bigger category of white-collar crime.

[57] HE 153/2006, Detailed Justifications, 3. Reasons of Governmental Bills, 3.2 Penal Code, Chapter 34 Endangerment.

revealed only with difficulty. On the other hand, trans-territorial crime becomes easy with the help of data processing systems, as compared with the traditional communications system and transportation system. Data processing systems integrate the function of many traditional systems, enabling a remote operation of communications, transportation, authentication, banking, printing, and so forth.

5. Raising multidisciplinary awareness. In the past, scholars attempted to label all those disciplines relating to crime by the term "criminal" and formed many interdisciplinary subjects, such as criminal psychology, criminal sociology, etc. The twentieth century development of criminal phenomena made it overcomplicated to generate so many disciplines. Rather than labelling informatics, cybernetics, etc., "criminal", scholars from different disciplines pursue research from their own standpoints. Works of many disciplines accommodate the contents of cyber ethics and cybercrime as inseparable constituent. Crime and its study are both more "cyber" than "criminal". Many criminalists migrated from the criminal sciences to other disciplines before the information age. Today, more non-criminalists are migrating from their own disciplines to the criminal sciences.

6. Holding the digital criminal power. While data processing systems utilise the power of the digital form, crime is also becoming digital. "Being digital"[58] means "being different" from the traditional social life. "Being digital" also means complexity and advancement of criminal circumstances. The power of information is expressed in digital form, both in social welfare and in social problems. It is natural for criminals to exploit the digital power of the scientific and technological advancement. In fact, the criminal phenomenon of the present day is modernised by the label of "being digital" in its spatiotemporal existence, with the emergence of new types of offences and new forms of old offences.

7. Continuing the vitality and continuity of the criminal tradition. Aggressive activities are universally acknowledged among animals. Crime is as old as human beings, who made the law to punish it. The cornerstones of criminal science are offences such as homicide, theft, robbery, arson, etc. The development of criminal phenomena demonstrates the continuity of tradition and the revision of minor details, including the tools used, the vehicle driven, the assets obtained or the premises destroyed. However, with interests and security as the basic goals, the foundation of criminal phenomena has not

[58] "Being digital" comes from the name of a book by Nicholas Negroponte (1995), who put forward a future vision of digital technology. See Nicholas Negroponte, *A Bill of Writes* (1 May 1995) Wired 3.05 <http://www.wired.com/1995/05/negroponte-18/>.

changed. Labelling a crime "cyber" is merely adding new factors to the tradition, but not undermining the innate foundation. With this label, traditional criminal law just takes a new step forward.

8. Corroborating the transformation of criminal patterns. If we say that the traditional criminal phenomenon was symbolised by forces and violence, the characteristic of cybercrime is the involvement of intelligence and intrigue. The physical and psychological existence of past human beings was confronted by threats of starting a bloody scene. Even in the present day, terrorist attacks are far more often the primary headlines in the mass media and a theme of critical concern for governments. The bloody scene remains a severe threat, but a silent transformation of this threat is happening with the continuing growth of data processing systems. Certainly, there is no sign demonstrating that the traditional fatal violence can be replaced by cybercrime or cyber terrorism. Cybercrime represents merely a tip of the iceberg of the entire crime scene.

VI ADVANTAGES OF A DEFINITION IN BROAD SENSE

Considering the previous experiences and lessons in legislation and law enforcement, a broad definition of cybercrime would have a number of advantages in criminal-law reform.

A broad definition of cybercrime would help to achieve as great a consensus as possible in the context of criminal-law reform. International negotiation is a prolonged and expensive process. A consensus based on a narrow definition would not be as effective as one based on a broad definition. Criminal justice according to a less consentient mechanism will inevitably meet unsolvable difficulties that require a new round of international consultation. Considering that current international consensus is inadequate, supplementary agreement is necessitated in the near future to acquire a broader coverage. An international treaty should be based on such a broad definition that member states would only exclude *by way of reservations* clauses unsuitable according to their own needs and traditions, but not exclude such contents from the treaty and hinder other states from accepting these clauses.

Additionally, a broad definition would help to revise criminal law completely, thus avoiding adding simply a couple of isolated articles. The isolated articles leave the cybercrimes in the broad sense unpunishable according to laws. The broader the coverage of the definition, the more possible it is for criminal laws to prescribe more activities as falling under the category. Many countries, including China and the US, initial laws with very limited coverage over activities or targets; however, they all subsequently made amendment so as to expand the scope of their legislation. Starting from a broad definition will

avoid the waste of legislative resources.

Again, a broad definition would help to amend procedural criminal law based on substantive criminal law. Without a qualified procedural law, the amendment of substantive law is easily invalidated. In the common law system, the division between procedural law and substantive law is not so clear. Nevertheless, in other legal systems, the coordination of these two branches of law has sometimes required a special legislative process. The prior enactment of substantive law is reasonable before procedural law. For both the substantive and procedural laws to be more effective and more consolidated, a broad definition of cybercrime would enable a better drafting of provisions in procedural law.

After all, a broad definition would also help to provide full protection for a critical information infrastructure. Legal science should always face the social changes that are seeking to influence legal notions and the legal framework. However, social changes have never happened so rapidly in history as they do today. Due to the trans-border nature, the development of cybercriminal phenomena is a particular example that must be considered from the global viewpoint.

VII COMPONENTS IN DEFINING CYBERCRIME

Now it is possible to define cybercrime as any type or any form of traditional or untraditional crime involving data processing systems in use as mass media, operating mechanism, place of occurrence, transfer channel, targeted object, multiple-purpose instrument, or used in the preparation for other crimes.

First, cybercrime covers any form of traditional or untraditional crime that can involve data processing systems. With the universal use of data processing systems, many types of new crimes emerge, many old crimes occur in new forms, and many new and old crimes happen interlinked. If data processing systems are the key factors in the crime, the crime falls into cybercrime. If an offence cannot be committed through data processing systems, it is not a cybercrime. According to the relationship between the cybercrimes and traditional crimes, cybercrimes can be divided into cybercrimes as substitutes for traditional crimes and cybercrimes as the complements of traditional crimes. The occurrence and increase of substitutes depend on the costs compared with traditional crimes. When the costs of cybercrimes are lower than traditional crimes, cybercrimes will increase, and vice versa. The occurrence and increase of complements, nevertheless, depends on the costs when compared with traditional crimes committed by other means. When costs of traditional crimes committed by the means of computers and

networks are lower, crimes of this kind will increase, and vice versa. In this sense, cybercrimes turn out to be traditional crimes facilitated by computers and networks.

Second, data processing systems are the distinct factor in cybercrime. Li proposed that a computer crime should be defined as a crime relating to "computer data processing systems".[59] Computer crime, or cybercrime, is by its nature information crime. The definition of cybercrime must contain the element of digital information or be a part of data processing systems. But computers and networks are simply the *present* representative of data processing systems to create, process, transmit, duplicate, exchange, disseminate, modify and destruct digital information. The hardware, software, and peripheral devices are only parts of these data processing systems. The development of ICT may simply outgrow the systems' current forms. Whatever the forms we use, however, such a mechanism as data processing systems will remain.

The terms "computer" or "network" cannot embody the complete scene of data processing systems, nor be expected to point necessarily to the future of the technology. Many of the previous definitions focused on "computer", and later definitions emphasised "network" as well. However, the image of computers and networks is changing; the transformation in the future may be faster and greater. It is reasonable to incorporate the term of "data processing systems" into the definition of cybercrime instead of using the terms of "computer" or "network".

In addition, data processing systems must be in use. Data processing systems not in use cannot facilitate a cybercrime. The term "in use" has to be understood in a broad sense. A computer is in use from the time it is purchased as a facility until the time when it is disused and disposed as cast-off. The transportation, installation, debugging, examination, reparation, and temporary switching off do not cancel the status of being in use. A paid order is enough to make a computer in use, because the expected use will influence the decision-making and productivity of the user. If such a computer were to be damaged and the schedule of adopting such a device delayed, or the expected benefit reduced, the loss to the user would be apparent. A network in use also has a similar meaning. Different stages in the whole process of being in use have a similar sense but are different in importance.

In some cases, however, computers are no more than entertainment equipment in a victim's everyday life. Where this is the case, the function of

[59] Li, above n 8.

the information processing of the computer is not particularly emphasised. Then, even if the computer is quite expensive, theft or destruction of it should not be regarded as a cybercrime. In KKO:2000:17, the accused, who was invited to the victim's house, took the victim's portable computer and other devices after the victim fell asleep.[60] In I-SHO 13.11.2006 1401, the accused usurped a portable computer valued at 880 euros from a shop and sold it to a man at the price of 70 euros, for he regarded it as a typewriter.[61] Although the movable property was valuable, nothing about the special function of the computers was mentioned in the courts. It is apparent that the offence was not committed against data processing systems "in use" for the purpose of information processing, and the loss was of such a nature as to be neglected compared with the value of the computers as commodities.

Furthermore, the roles of data processing systems in cybercrime are multiple. Data processing systems can be exploited as mass media, operating mechanism, place of occurrence, transfer channel, targeted object, multiple-purpose instrument of a crime, or used in the preparation of other crimes. As explosives are different from primitive weapons, a plane different from other vehicles, data processing systems are different from many traditional facilities. The accompanying conceptions are data processing and transmission, multimedia, virtual reality, remote control, online interactive, and so forth. With data processing systems, people are involved in intersensory actions. To evaluate the functions of (current and future) data processing systems is a matter that cannot be overestimated. The equivalent applies to the situation of cybercrime, which is committed intersensorily.

Finally, it is also necessary to point out that, even if we adopt a broad definition of cybercrime, the offences merely involving data processing systems but having nothing to do with their functions do not constitute cybercrime. A typical example is the prohibition of import or export of computers, software, or technology. Many countries have trade prohibitions of this kind so as to maintain the political, military, or scientific competitive priority, and this might mean even limiting the public from using such devices. For example, according to the Myanmar Computer Science Development Law of 1996, the importing, keeping in possession or utilising of any type of computer, or setting up a computer network or connecting a link inside the computer network, without prior sanction, are offences punishable by imprisonment of 7 to 15 years and a fine. Offences of this kind do not belong to cybercrime in terms of this article.

---

[60] Supreme Court Precedent of Finland, KKO: 2000:17.
[61] High Court Precedent of East Finland, I-SHO 13.11.2006 1401.

VIII CONCLUSION

The phenomenon of cybercrime is comprised of a complex of acts and facts, which are multifarious, concealed and changing, missing a ready-made theory applicable for defining and categorising various practical cases. A great many disputes exist as to what exactly constitutes a cybercrime, for there is a lack of an internationally recognised criterion, which results in conflicts in trans-national law enforcement and a waste of judicial resources.

Virtual Courts – A Fundamental Change to How Courts Operate

Keith B Kaplan*

A virtual court is a conceptual idea of an online judicial forum that has no physical presence, but still provides the same justice services that are available in courthouses.[1] Virtual courts are becoming a reality, in part, in many venues as litigants expect more accessibility to courts without having to be physically present. While many courts are beginning to adopt technology to remove the barrier of physically having to be present, courts face significant challenges when attempting to exist solely in a virtual environment.

I COURTS MOVING TOWARDS VIRTUAL ACCESS

Many courts are moving towards becoming virtual, at least in part, to allow for greater accessibility, functionality, and cost-savings. Fountain Hills Municipal Court, a limited jurisdiction court in the Phoenix Metropolitan area (Arizona, United States), has implemented video arraignments for all in-custody defendants. In lieu of transporting in-custody defendants over thirty miles (48 km) to be seen before a judge, defendants are brought to a special jail cell that has a computer with a video camera. A judge sits at his/her desk or bench inside the courtroom and arraigns in-custody defendants by video without having them physically present. This has resulted in transportation cost savings and has reduced the time defendants remain in-custody since they no longer have to be transported to the courthouse.

II WHAT THE FUTURE HOLDS

Courts are rooted in tradition and many technology decisions are made based on those traditions. While courts use of technology may evolve slowly, courts can look beyond what is currently available in the public sector to conceptualise and develop technology to further enhance accessibility and to meet public expectations.

---

* Assistant Court Administrator, Phoenix Municipal Court.

1 Keith Kaplan, 'Will Virtual Courts Create Courthouse Relics?' (2013) 52(2) *The Judges' Journal* 32, 32.

Nearly three-quarters of adults in the United States have smartphones.[2] Eighty-six percent of American adults between the ages of 18-29 own smartphones, as do 83% of those between the ages of 30-49.[3] With a mobile computer at the hands of most Americans, there is an expectation and demand that litigants should be able to utilize this technology to virtually access courts, just as they would access other services from their phones. Courts should not shy away from their constituents' desires to remotely access courts, especially if it will result in court resource savings while still maintaining the principles of justice courts are built upon.

One example of virtualising courts by way of mobile devices (phones and tablets) is for courts to develop applications ("apps") for litigants and stakeholders to download to their phones. Some functions courts may want to include are: parking and map directions, contact information, electronic filing (e-filing), video capability to appear remotely by phone, way-finding information for inside the court, and the ability to receive assistance from court staff. An example of courts moving in this direction are the New Jersey State Courts which have developed a mobile phone app for jurors that provides jury service information, maps and driving information, and juror check-in capability.[4]

Courts should also strive to allow for video interaction between court staff and people needing assistance by way of their mobile devices. The online store Amazon introduced "Mayday" to allow users of their Fire tablets to access an Amazon Tech advisor 24 hours a day, seven days a week, 365 days a year for free.[5] Mayday allows users to see a tech advisor and ask questions, but the tech advisor can only see the users screen.[6] With the virtualisation of courts leading to less physical traffic entering physical courthouses, courts can allocate their resources to staffing video chat support to provide assistance to people virtually accessing the court. Due to resource constraints, courts may only want to provide this service during normal hours of operation. This will allow courts to provide in-person virtual assistance to those virtually accessing the court.

---

[2] Monica Anderson, *Technology Device Ownership: 2015* (29 October 2015) Pew Research Center <http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/>.
[3] Ibid.
[4] See Stuart Rabner, 'Using Technology to Improve Jury Service' [2014] *Trends in State Courts* 39 <http://www.ncsc.org/~/media/Microsites/Files/Future%20Trends %202014/Using%20Technology%20to%20Improve%20Jury%20Service_Rabner.ashx>.
[5] Amazon Mayday is a product offered by Amazon.com, Inc. on Amazon Fire tablet devices allowing technical service advisors to access a tablet at the push of the Mayday button. See Amazon, *Mayday: Get Help on Your Fire Tablet* (2016) <http://www.amazon.com/ gp/help/customer/display.html?nodeId=201540070>.
[6] Ibid.

III OVERCOMING THE CONSTRAINTS OF VIRTUAL ACCESS

For many jurists, there are concerns with being able to see and read expressions and body language from people appearing by video.[7] As video technology improves, this is less of a concern as long as there is two-way high-definition video (video seen by both sides).[8] Another way courts can address this is to implement virtual reality, creating an immersive multimedia court appearance.[9] Virtual reality is computer technology that simulates an environment and a user's physical presence in a way that allows the user to interact with it creating a sensory experience, which can include "virtualsight [sic], sound, smell, taste and touch."[10] Virtual reality can completely change the way litigants interact with courts.

Virtual reality may eliminate the concerns courts have with litigants virtually accessing courts because litigants and attorneys will be able to be virtually present from a remote location and simulate their physical presence in court. Virtual reality and the associated technology will allow for the replication of a physical courthouse in a virtual space. With the integration of e-filing, litigants and their attorneys are now able to file documents immediately upon the court's request; this will further simulate a litigant's physical presence in court. Virtual reality and related technology will allow courts to overcome some constraints of virtual access.

Another option similar to virtual reality is augmented reality or the viewing of a physical, real-world environment from which "elements are augmented by computer-generated sensory input such as sound, video, graphics, or GPS data."[11] Augmented reality allows users to view virtual computer-generated images or graphics overlaying real-life images as opposed to a fully simulated virtual reality. Augmented reality would allow users to view live images inside courtrooms, but overlay those images with computer-generated inputs. This would go beyond virtual reality, which simply simulates an environment, by making users feel as if they are actually present and able to handle documents and move throughout a real courtroom. Augmented reality will allow users to interact and feel present in an actual courtroom by viewing a live video feed of court proceedings and interacting with their surroundings.

---

[7] Jacqueline Horan, *Juries in the 21st Century* (Federation Press, 2012) 139.
[8] Ibid 140.
[9] Fei Hu, Jiang Lu and Ting Zhang, *Virtual Reality Enhanced Robotic Systems for Disability Rehabilitation* (Medical Information Science Reference, 2016) 49.
[10] Ibid.
[11] Space and Naval Warfare Systems Command, *Battlespace Exploitation of Mixed Reality (BEMR) Laboratory: Technologies* <http://www.public.navy.mil/spawar/Pacific/BEMR/Pages/Technologies.aspx>.

Whereas virtual reality and augmented reality are developed to a level where they are being implemented now, holographic technology may offer an option in the future to create a space with three-dimensional representations of all persons "present." An example of this is a room setup as a traditional courtroom where holographic representations of everyone involved are present to participate in court proceedings. While holographic imagery is in its infancy and may never evolve into a viable technology, this may create a more realistic virtual court setting.

When moving to a virtual court, courts as institutions must decide why and what they are trying to accomplish. If courts are trying to eliminate the need for physical courthouses, virtual reality may be the most viable option as a simulated courthouse could, in theory, be developed to mimic the physical presence of a courthouse and courtroom proceedings. If courthouses are still planning on being utilised but only requiring people to appear by video, augmented reality may be the best option as it will show a live feed of the court proceedings and each participant will be "present" by video, but there can be greater interaction between persons than with a standard video presence. Holographic technology may provide a medium where it appears individuals are participating live and in three-dimensions, but the proceedings are actually occurring in a simulated virtual space.

While the technology currently exists to utilise virtual and augmented realities and the potential exists to implement these technologies in courts, the biggest issue courts will face if they choose to implement this technology is the development of the virtual spaces and other content programming requirements. Courts would need to create virtual courtrooms that meet their needs and ensure quality justice services. A lot of development would need to go into these virtual spaces in addition to the content delivery to all users. Thus, while courts may not be prepared to move to the virtual space in the near future, they should begin planning to explore the possible implementation of these technologies in the future.

IV MOVING BEYOND TRADITIONAL COURT JURISDICTIONS

What if transitioning to virtual courts allowed litigants to access any court at any time? Are courts and legislatures prepared to remove jurisdictional boundaries in counties, states, and even countries to provide greater access? With the idea of virtual courts eliminating the need for physical courthouses, it is possible for litigants to access any court at any time. This may make more sense applied within a single state in the United States since state laws govern and the courts will be versed in those laws, rules, and regulations. This may also work better in unified court systems where all courts in that system are

administratively consolidated into one court system.[12] However, as courts potentially adopt a virtual court process, more states may elect to transition to unified or tightly integrated court systems to allow the public to access any court in that state for any reason. Generally, unified court systems are also centrally funded, which allows these court systems to centrally determine funding allocation to courts based on litigant utilisation.

A positive outcome of a unified virtual court system is that courts can develop technology to route filings, assistance requests, and other processes that require processing and work by court staff and judges equally among all courts. This should reduce wait times and backlog and delay in the larger metropolitan areas since cases will be distributed equally amongst court locations. However, this may require more staff to process cases in rural areas which may result in court systems electing to keep courts the same size they currently are and distribute cases using a system that gives larger courts more cases. However, this line of thinking still requires courts across states to exist; with virtual courts, there needs to be a shift in how courts and the public think about court jurisdictions.

Minnesota's Court Payment Center is an example of a unified virtual court. Established in 2009, the Court Payment Center "streamline[s] the processing of citations, offer[s] cost-effective, convenient and alternative methods of service, and mobilise[s] technology and automation" to improve the processing of citations.[13] While not a court in the traditional sense, the Court Payment Center is a "centralized, statewide operation for traffic case processing that leverages automation and technology, optimizes economies of scale, reduces labor costs, and augments service-delivery options for court customers." [14] As of 2015, the Court Payment Center processed 1.3 million citations annually, resulting in $100 million in revenue.[15] By moving beyond traditional court environments, Minnesota has become more efficient in case processing, improved delivery of services by allowing 24/7 access, and they have centralised operations while decentralising staff to create operational successes.[16]

---

[12] *Facts You Did Not Know About the Unified Court System* (2015) Laws.com <http://court.laws.com/unified-court-system>.

[13] Minnesota Judicial Branch, *Pay Fines FAQs* (2016) <http://www.mncourts.gov/Pay-a-Fine.aspx#tab03FAQ>.

[14] National Center for State Courts, *Court Technology Conference Track 5: Streamlining Traffic Case Processing* (2015) <http://www.ctc2015.org/Education-Program/Tuesday/Morning/Session-2/Streamlining-Traffic-Case-Processing.aspx>.

[15] Ibid.

[16] Rebecca Becker, *Streamlining Traffic Case Processing: Minnesota's Opportunity* (Minnesota State Court Administrator's Office, 2015) <http://www.ctc2015.org/~/media/Microsites/Files/CTC2015/Materials/1115-Tues-Track-5-Streamlining-Traffic-Case-Processing.ashx>.

One option to be more efficient and save money is to have one centralised court for each state that processes all cases and interacts via video and virtual reality. With this model, there will no longer need to be physical courthouses throughout the state to provide local access to litigants. Courts will exist largely as legislatures exist and will be situated in the capitol city alongside state legislatures. This model requires courts and the public to change their mindset about every aspect of the courts.

Judicial selection and determining representation from different parts of the state will also need to be addressed. One option is to elect judges similar to how legislators are elected. Others may appoint judges only in the location where the court is situated because they will be required to preside over cases in that area. However, with virtual courts allowing virtual access by defendants, some courts may decide to allow judges and staff to work remotely and access their court's work virtually. This will allow judges to still preside over cases while serving different areas and jurisdictions of the state. In order to take those local interests into account, courts may decide to distribute cases to judges based on the filing location of the parties and the location of the judge presiding over cases in that area. In theory, judges could be located anywhere, but state legislatures and courts may decide to contain jurisdictions and workloads within their respective states.

This idea of virtualising courts and distributing cases could extend to Federal courts. Similar to state courts, Federal courts may elect to eliminate physical courthouses and distribute cases to judges based on caseload. A judge in Phoenix may preside over a case with parties residing in New York. Virtual courts eliminate the barriers that physical courthouses suffer from; expanding how everyone thinks about courts can make them more accessible.

V CHALLENGES AND ACCESSIBILITY

While automating the courts and allowing virtual access is an achievable goal in the near future, will virtual courts actually improve access to courts and reduce their costs? While most Americans have mobile devices and desire remote access to the courts, a large amount of people still do not have the necessary hardware to access virtual courts. Courts should not restrict nor eliminate access because a person does not have the required technology to access virtual courts. Courts should strive to improve access; while improving access to people with the required technology, automation and virtualisation of the courts may create more barriers the courts must overcome to be successful in transitioning to virtual access. Since courts are government institutions that exist to protect individual rights and liberties, they need to be accessible to

everyone.[17] Courts may initially look to create a virtual presence only for litigants represented by attorneys.

A challenge when implementing changes to court processes is to determine if those changes should be done incrementally or all-at-once. By initially restricting access to virtual courts to attorney represented cases and for specific case types, courts will have separate processes for virtual access and physical access to the court. This will be burdensome and will require additional staff, something transitioning to virtual courts will help eliminate. Courts that choose this route will likely add more case types and open up virtual access to unrepresented litigants subsequent to the initial limited implementation. This piecemeal process of transitioning to virtual courts will help courts remain accessible, but will also make processing the caseload as a whole more difficult for the courts.

Courts are different than private sector businesses as courts must remain open and accessible to everyone.[18] In order to allow individuals without access to the technology required to access virtual courts, courts must provide solutions to those individuals. Another option for virtual court access is to have courts develop kiosks or remote access stations that give litigants and members of the public the ability to utilise virtual technology to access courts. These kiosks can be setup as stations, either inside the courthouse or at remote locations, to provide litigants the tools required to access courts. Courts will likely have to develop new interfaces to work in conjunction with mobile application technology to successfully implement these kiosks. An alternative to standard computer stations would be to use secured tablets loaded with the court's mobile application. This option will provide the same user interface as a mobile phone and will reduce the amount of support required if separate interfaces are developed. Similarly, if courts expect people to utilise virtual reality to access courts, courts will need to provide this technology to be utilised by litigants without access to virtual reality devices.

---

[17] The purposes and traditional roles of courts are covered in detail in the Institute for Court Management's class on The Purposes and Responsibilities of Courts, which included Ernie Friesen's Eight Purposes of Courts: Ernie Friesen, *Core Competency Fundamentals: Purposes and Responsibilities of Courts* (National Association for Court Management, 2007). Retrieved from <http://www.nacmnet.org/sites/default/files/CCCG/toolboxes/powerpoint/Purposes_2.5%20Day_Slides.ppt>.

[18] Ibid.

VI CONCLUSIONS

Virtual courts, or concepts that virtual courts are built upon, are beginning to be implemented in courts around the world.[19] Courts are beginning to realise the benefits that technology and automation can provide to increase accessibility, efficiency, efficacy, and cost savings. When deciding to implement more technology to create virtual courts and remove physical access, courts should consult with the community and other stakeholders to determine which path is the best for them. As the public and stakeholders become accustomed to accessibility through technology, they have come to expect this level of service and access from the courts.

Courts should begin researching and deploying mobile application technology, virtual reality, and other virtual court technology to prepare for a shift in mindset of how the public and stakeholders expect to access courts. A change in mindset of court leaders, judges, and court staff will also be required to change business processes and move away from traditions to become more accepting of virtual courts to meet the demands of constituents and stakeholders.

---

[19] Fountain Hills, Arizona and other courts across Arizona are implementing video conference technology to arraign in-custody defendants by video, and the Arizona State Judiciary is utilizing video for remote interpreter services: see Arizona Judicial Branch, *Video Remote Interpreting* (2016) <http://www.azcourts.gov/interpreter/Video-Remote-Interpreting>.

In addition, courts in Kent, United Kingdom, have implemented "virtual courts" to allow defendants to appear for their first hearing by video from the police station: see *'Virtual' courts rolled out across Kent* (1 August 2012) BBC (Online) <http://www.bbc.com/news/uk-england-kent-19080208>.

The Legal Profession Disrupt

Fabian Horton*

I PRACTISING IN A DISRUPTED PROFESSION

In the 2011 movie *The Lincoln Lawyer*, Matthew McConaughey plays the role of a lawyer who operates his practice out of the back of his car (a Lincoln Continental sedan). While this depiction is very much a product of the Hollywoodisation of lawyers, it serves well as a metaphor of modern practice and the disruption that is taking place. The concept of the lawyer who is mobile, without a fixed address, and who meets with the clients where convenient, is one that is representative of a growing number of legal practices. It constitutes a way of practising that is in contrast to the traditional model where the bricks and mortar office is the symbol of the lawyer's profession, where the way that the lawyer interacts with the client, usually through face-to-face meetings and letters, has been the same for decades, if not centuries.

II THE TECHNOLOGY IMPERATIVE

Practising law in this time of change and into the future is going to take a reconceptualising of how lawyers not only manage the profession of law, but also the business of the provision of legal services. Understanding this evolving state of legal practice requires an understanding of the context in which it is occurring. The proliferation and uptake of enabling technologies has been identified in some commentaries as the 'Fourth Industrial Revolution'.[1] This revolution (or disruption) has both its socio-economic[2] and technological drivers of change.[3] At the core of the technological drivers is that of hyperconnectivity.[4] In this context, hyperconnectivity represents a wide group

---

* Solicitor, B.Mus, LL.B. LL.M.(Hons), PhD Candidate (SCU).

[1] World Economic Forum, 'The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution' (Report, January 2016) < http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf >. See also Klaus Schwab, *The Fourth Industrial Revolution* (World Economic Forum, 2016); Gideon Rose, *The Fourth Industrial Revolution: A Davos Reader* (Council on Foreign Relations, 2016).

[2] World Economic Forum, 'The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution' (Report, January 2016) 5 <http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf>.

[3] I would argue that the technological drivers are also the primary influences in the change in socio-economic conditions that are leading to the changes in business models. See ibid 6 for a list of the technological drivers.

[4] It is important to note that being connected to broadband Internet does not necessarily denote hyperconnectedness. Hyperconnectivity is more than just sending messages or talking to each

of information and communication technologies that include mobile technologies, internet and cloud technologies, and technologies such as virtual and augmented reality.[5] It is these technologies that have enabled a range of legal service providers to reconceptualise the way they undertake the day-to-day work of legal practice, and the way that they structure themselves as service providers. Hyperconnectivity lays open the domains of knowledge that was once the sole province of lawyers. The worldwide digitalisation and spread of that knowledge and information has opened the once vigilantly guarded legal sanctum to disruption in both form and function.

III THE CONNECTED LAWYER

Every aspect of how the lawyer undertakes tasks and performs duties is being reimagined in the digital space. By connecting information repositories and allowing for distributed collaboration, the lawyer is no longer tied to the protocols and formalities of the analogue (paper) world. Content and precedent management systems are now firmly entrenched within the legal office. Many of these systems automate the production of documents for the lawyer and the client. The move to online cloud-based systems (including for accounting and billing purposes) means that lawyers can now remotely access their information (files) and manage their matters and practice wherever they can get the Internet. The emergence of digital assistants and artificial intelligence[6] is now seeing basic, routine tasks move from the lawyer to the machine.[7]

These moves away from the somewhat laborious, analogue exertions have however been ongoing for many years. Digitised online (and in many situations free) access to legislation and case law[8] could be argued as one of the original

---

other or even seeing each other in moving images. That kind of connectivity already exists through earlier technologies such as the telegraph, the telephone, radio and television. Hyperconnectivity incorporates elements such as multiple channels, connectivity through multiple devices and the ability to be constantly connected.

[5] Other technologies such as artificial intelligence, big data and analytics are also assisting in this regard. I argue that hyperconnectivity underpins these technologies as it is the internet that is, for the most part, their enabling technology.

[6] Consider the Apple technology Siri and the Google technology Google Assistant. See: Matthew Lynley *Google unveils Google Assistant, a virtual assistant that's a big upgrade to Google Now* (19 May 2016) Techcrunch <https://techcrunch.com/2016/05/18/google-unveils-google-assistant-a-big-upgrade-to-google-now/>.

[7] For a more general and somewhat amusing discussion on the virtual assistants see: Alford Henry. *Dawn of the Virtual Assistant* (25 June 2016) The New York Times (Online) <http://www.nytimes.com/2016/06/26/fashion/technology-artificial-intelligence.html>.

[8] For example, for information about the online legal materials publisher AustLII, see: <http://www.austlii.edu.au/austlii/>. Also see: Graham Greenleaf, 'Free access to legal

disruptors in the legal field. Access to primary legal materials has long been the sole domain of the lawyer. Now any person with access to the internet and Google can find legislation or case law. Most of the popular legal databases have full text search functions,[9] saving time when searching for specific materials in what was once an extremely time consuming exercise. The next step in the development of this technology focuses on the use of artificial intelligence. With the use of content analytics and natural language processing legal[10] publishers are continuing to capitalise on machine power to assist lawyers in both reviewing legal information and producing evidence-based legal solutions and strategies; both of which were once the sole domain of the lawyer.

The disruption caused by digitised legal information is not just limited to lawyer tasks and this is having an effect on how the lawyer interacts with the client. Online legal information now means that specific legal materials can be found without the user having an intricate knowledge of the legal research protocols.[11] And while non-lawyers may not fully understand the information presented, the trend of free online legal information continues with the proliferation of secondary legal materials that can assist in comprehension. There is also now a plethora of legal opinions and analyses, often written by law firms themselves, which are available for the education of the reader.[12] So while it was once the domain of the lawyer to inform the client about the law, clients are becoming more adept at researching their own legal problems on the internet and are now better informed as to their situation before they come to the lawyer. While there are still complexities requiring professional legal assistance, we are now seeing a more informed and sophisticated client. In addition, with the increasing number of in-house lawyers, corporate clients are becoming increasingly astute consumers. The end result is that the regurgitation of legal information is a product that clients are less likely to want

---

information, LIIs, and the Free Access to Law Movement' [2011] *University of New South Wales Faculty of Law Research Series* 40.

[9] For example, AustLII, LexisNexis and WestLaw legal research systems all have advance full text search facilities.

[10] See Thomson Reuters Corporation, 'Thomson Reuters and IBM Collaborate to Deliver Watson Cognitive Computing Technology' (Press Release, 8 October 2015).

[11] For example, see FoolKit Website, *for the public* <http://www.foolkit.com.au/vic/public>; Duke University *Legal Research for Non-Lawyers* (July 2015) Duke Law (Online) <https://law.duke.edu/lib/researchguides/nonlaw/>; American Association of Law Libraries, *How to Research a Legal Problem: A Guide for Non-Lawyers* <http://www.aallnet.org/mm/Publications/products/How-To-Research-A-Legal-Problem/howtoresearchlegalproblem.pdf>.

[12] See Ellie Margolis, 'Authority Without Borders: The World Wide Web and the Delegalization of Law' (2011) 41 *Seton Hall Law Review* 909; Robert J Brown Jr, 'Essay: Law Faculty Blogs and Disruptive Innovation' (2012) 2 *Journal of Law (Journal of Legal Metrics)* 525.

to pay for. Lawyers must now be keenly aware of the heightened importance of the analytical problem solving skillset that the consumer is requiring of them.

Another move to the digital realm that is disrupting the status quo is the introduction of such facilities as the PEXA[13] conveyancing system. In 2016 the first paperless conveyance went through in New South Wales.[14] This represents a wholesale change in procedure for what is a centuries old system of regulation and authentication of land title holdings and dealings. This, however, is merely the start of the disruption that could occur in this area. Blockchain[15] (or at least some variation on this theme) is poised to reconceptualise land dealings and registration.[16] Countries such as Honduras,[17] Sweden[18] and the Republic of Georgia[19] all have reportedly commenced investigating blockchain land registry systems that have the potential to either upgrade or replace legacy systems with one database.[20] This demonstrates the high potential for technology to effect wholesale change in the way transactional matters are conducted and to supplant the requirement for lawyers to participate in the process.

The resolution of disputes is also being disrupted with the emergence of new online process which have outstripped earlier systems with the enhanced capacity and functionality that digital platforms offer.[21] The lack of lawyer

---

[13] Property Exchange Australia Ltd, *PEXA* <https://www.pexa.com.au/>.

[14] Su-Lin Tan, 'Paperless apartment sale in Sydney suburb makes history', *Sydney Morning Herald* (online), 9 June 2016 <http://www.afr.com/real-estate/paperless-apartment-sale-in-sydney-suburb-makes-history-20160530-gp7kr2>.

[15] Also known as Distributed Legal Technology.

[16] See Alex Liebenau Mizrahi. *A blockchain-based property ownership recording system* <http://chromaway.com/papers/A-blockchain-based-property-registry.pdf>; Jonathan Liebenau and Silvia Monica Elaluf-Calderwood, *Blockchain Innovation Beyond Bitcoin and Banking* (18 March 2016) <http://ssrn.com/abstract=2749890>.

[17] Gertrude Chavez-Dreyfuss, 'Honduras to build land title registry using bitcoin technology', *Reuters* (online), 15 May 2015 <http://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515>.

[18] Gertrude Chavez-Dreyfuss, 'Sweden tests blockchain technology for land registry', *Reuters* (online), 20 June 2016 <http://www.reuters.com/article/usswedenblockchainidUSKCN0Z22KV>.

[19] Laura Shin, 'Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury', *Forbes* (online), 21 April 2016 <http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury>.

[20] For an explanation of the issues see Alex Mizrahi, 'A blockchain-based property ownership recording system' (Whitepaper, Chromaway, 2015) <http://chromaway.com/papers/A-blockchain-based-property-registry.pdf>.

[21] Online Dispute Resolution (ODR) has been in development for many years and in by some measures is now a mature proposition. See Thomas Schultz, 'The Roles of Dispute Settlement

intervention at this level of dispute resolution (both in the real world and online) is both a reflection on the amount of disputes that are dealt with and generally the lower quantum of the dispute. Recognising the need for a technological intervention in low-value disputes, Lord Justice Briggs of the Court of Appeal of England and Wales has recommended the creation of an online court which would be the compulsory starting point for money claims worth up to £25,000, and which will be designed "for navigation by litigants without lawyers".[22] This is in line with the recommendations made earlier by English Civil Justice Council report for an online court for small monetary claims[23] chaired by academic and commentator Richard Susskind. While the extent of this type of court is currently limited to matters which, in many situations, wouldn't see the intervention of lawyers anyway, the trend of digitising the elements of disputes to then be dealt with virtually will continue. Even if this version of online dispute resolution does not occur, Lord Justice Briggs' report is a watershed moment. It shows that this type of thinking is now mainstream and coming from the institution of law. It is no longer a fringe consideration of a small group of tech-lawyers. Consequently, lawyers will need to carefully consider these technological developments and keep abreast with the changing requirements of assisting clients in the digital realm and be prepared to eventually appear in matters that are dealt with virtually.

The de-centralised, virtual operation of legal services has also moved into the human collaboration space. While mobile telephones have been a primary business tools for many years, advancements in video conferencing is seeing lawyers already successfully operate in this space. The traditional meeting with the client is now being replaced with online meetings spaces[24] or no meeting at all, with the use of interactive legal chat bots.[25] As consumers continue to be more reliant, or at least attracted, to mediating their communications through the online means, lawyers will have to be more open to using these technologies to service their clients in an appropriate and appealing manner.

---

and ODR' in Arnold Ingen-Housz (ed), *ADR in Business: Practice and Issues Across Countries and Cultures* (Kluwer, 2011) 135. For a selection of case studies see Pablo Cortes, 'Online dispute resolution services: a selected number of case studies' (2014) 20(6) *Computer and Telecommunications Law Review* 172.

[22] See Lord Justice Briggs, 'Civil Courts Structure Review: Final Report' (Judiciary Review, Judiciary of England and Wales, July 2016) 51 <https://www.judiciary.gov.uk/wp-content/uploads/2016/07/civil-courts-structure-review-final-report-jul-16-final-1.pdf>.

[23] See Online Dispute Resolution Advisory Group, 'Online Dispute Resolution For Low Value Civil Claims' (Report, Civil Justice Council, February 2015) <https://www.judiciary.gov.uk/reviews/online-dispute-resolution/odr-report-february-2015/>.

[24] For example, see the online collaboration space 'Legaler' at <http://home.legaler.com/>.

[25] An example is the legal chat bot Lexi who can be used to generate a free privacy policy. See Lexi at Lawpath, *Meet Lexi* <https://try.lawpath.com.au/privacy-bot/>.

IV THE BUSINESS COMPETITIVE

This new way of practising is part of the continued stratification of legal practice business models that has been ongoing for many years. Enabled by the forces of technology and the flexibility that it brings, lawyers are facing the pressure of practising in what is now being described as the 'gig economy'.[26] For those still in the mind frame of the traditional 'big firm, medium firm, small firm' structure, practising within this landscape can be confusing. This is not surprising as the technological imperative that is overtaking the traditional law firm model means that incumbents and new entrants alike are pressured to conform to a new paradigm. A paradigm that is demonstrative of the disruption that is taking place in the practise and provision of the legal services and one that sees a reformulation of the legal services models.

There is an inextricable link between the rise of these new classes of technologies and the rise of new forms of delivering legal services. The law firm has been traditionally categorised by its size. This in many ways reflected the type of clients that they attracted. Large city firms were renowned for having large corporate and high-net worth individuals as clients. Accordingly large firms employed the people and the resources to conduct large matters and complex cases. Furthermore the large firms had the capital to attract, train and retain top legal talent. This talent then perpetuated the large law firm partnership business model as they worked towards and bought into equity ownership.[27] Small and medium sized law firms operated in a similar fashion and this was reflected in the type of client that they attracted. The sole practitioner would invariably attract clients according to his or her particular skillset or location, and looked to build equity that could be later sold to another operator. Other forms of legal practices such as Community Legal Centres and special purpose law centres exist and operate within their mandate and budget constraints.

---

[26] The 'gig economy', also described as the 'Uber economy', is the economic and social activity of temporary positions and short-term engagements with independent workers. See Valerio De Stefano, 'The Rise of the "Just-in-Time Workforce": On-Demand Work, Crowdwork and Labour Protection in the "Gig-Economy" (2016) 37(3) *Comparative Labor Law & Policy Journal* 471; Antonio Aloisi, 'Commoditized Workers: Case Study Research on Labour Law Issues Arising from a Set of "On-Demand/Gig Economy" Platforms' (2016) 37(3) *Comparative Labor Law & Policy Journal* 653.

[27] George Beaton, *NewLaw New Rules - A conversation about the future of the legal services industry* (Beaton Capitol, 2013) 30. See also an opinion of the partnership business law firm models by industry commentator: Jordan Furlong, *The endangered partner* (28 July 2016) Law21 Blog <http://www.law21.ca/2016/07/the-endangered-partner/>.

The traditional model of operating legal services however is now consistently under challenge and is increasingly the subject of legal business analysis.[28] Referred to as BigLaw[29] (traditional firm model) versus NewLaw, NewLaw has been described as 'any strategy, structure, model, process, or way of delivering legal services that represents a significantly different approach to the creation or provision of legal services than what the legal profession has traditionally employed'.[30] The types of law firms that are representative of the NewLaw model include: dispersed law firms, lawyer placement agencies, virtual firms, online document retailer firms and fixed fee firms.[31] All, except the last category, represent models that have a reliance on technology (in a non-traditional sense). This is evidence of the increasing reliance of technology in the operation of modern law firms, especially for those who are newer entrants into the market. Consequently, it underscores the critical need for lawyers to understand the technological drivers of change if they are going to effectively participate in providing modern legal services.

V CONCLUSION

The world will continue to become increasingly hyperconnected as we incorporate more technology into our lives and as we do so in ways of increasing variety. As such the evolution/disruption of legal practice and legal business models will be ongoing. It will be the ability to be connected, mobile, accessible and agile that will benchmark the new imperative to be a technologically competent lawyer. The capacity to recreate from the most basic level upwards all facets of client interactions is seeing the redefining of the practice of law and the legal services business models.

As far as digital and technological literacy is concerned, lawyers will be required to know about technology so that they are able to properly service their clients in this new professional and business reality. As many of these skills are yet to be defined this is going to be a difficult task. With a legal

---

[28] Beaton above n 28. See also: Richard Susskind, *The End of Lawyers? Rethinking the nature of legal services* (Oxford University Press, 2010).

[29] George Beaton, *Last days of the BigLaw business model?* (6 September 2013) Beaton Capital *Bigger, Better, Both?* blog <http://www.beatoncapital.com/2013/09/last-days-biglaw-business-model/>.

[30] Jordan Furlong and Sean Larken, *A Brief Inventory of NewLaw in Australia* (25 August 2014) Australian Legal Practice Manager's Blog *A Survival Guide for Legal Practice Managers* <http://www.alpma.com.au/a-survival-guide-for-legal-practice-managers/inventory-of-new-law-in-Australia>. The term 'NewLaw' was originally coined by Eric Chan in describing certain new business models: see Eric Chan, *2018: The year Axiom becomes the world's largest legal services firm* (13 September 2013) Beaton Capital *Bigger, Better, Both?* blog <http://www.beatoncapital.com/2013/09/2018-year-axiom-becomes-worlds-largest-legal-services-firm/>.

[31] Marcus McCarthy, *NewLaw: What is it and why is it?* (27 March 2015) Lawyers Weekly <http://www.lawyersweekly.com.au/blogs/16322newlawwhatisitandwhyisit?>.

education system that is wedded to analogue, paper-based work patterns, lawyers must either be self-taught or seek out the skills through trusted advisors. If lawyers do not obtain a good understanding of the technology that is affecting their profession they risk becoming superseded by legal business propositions that are more relevant to today's clients and more agile so as to keep up with changing demands.

A Proposed Convention on Electronic Evidence

Stephen Mason*

The draft Convention on Electronic Evidence is the first attempt to prepare a text on electronic evidence that crosses jurisdictional boundaries. It deals with the status of electronic evidence; the investigation and examination of electronic evidence, and sets out a number of general provisions regarding the recognition and admissibility of electronic evidence from foreign jurisdictions. The main objective of the Convention is to pursue a common policy towards electronic evidence, taking into account the differences in the treatment of evidence in individual jurisdictions. Another aim is to encourage judges and lawyers to more fully understand the concept of electronic evidence in the interests of providing for fairness in legal proceedings; to promote adequate legal procedures; to implement appropriate legislation where necessary and to promote international co-operation.

I THE IDEA OF A CONVENTION ON ELECTRONIC EVIDENCE

I have undertaken a great deal of training of judges and lawyers in electronic evidence across the world (India, Tanzania, Thailand, Tonga, United Arab Emirates), and with the Academy of European Law in Europe (Bulgaria, Cyprus, Czech Republic, England, Estonia, France, Germany, Italy, Latvia, Norway, Portugal, Romania, Spain, Turkey, Ukraine). More recently, participants have asked if the United Nations or the Council of Europe were considering a Convention on Electronic Evidence.

I am not aware that either body is considering such a Convention. This could be because at the political level there is no interest, and possibly because such a Convention might take some years to develop to the satisfaction of all the parties. I appreciate that drafting such a Convention at the international level between governments needs to include political considerations. I do not wish to make light of this aspect of negotiations, because it is important. However, given that we now live in a networked world, and people do horrible things online, I think it is important to encourage politicians and commercial legal entities to understand that the flow of electronic evidence, especially between prosecutors across legal boundaries, is important for a number of reasons: the successful prosecution of people that have done something seriously wrong and where they have caused loss, harm and distress to innocent victims, and

* Barrister-at-law, United Kingdom Bar, BA (Hons) (History and Educational Philosophy), MA, LLM, PGCE (FE).

for the social stability of nation states.

In the absence of a discussion of the development of such a Convention at an international level, I concluded that it might be useful to develop such a Convention with the help of judges, lawyers and other interested individuals across the world. I appreciate this is a private initiative, but sometimes private initiatives help. I discussed the methods by which a convention might be considered in a lecture I gave on the topic at the Faculdade de Direito in the Universidade de Lisboa on 4 March 2016, and followed this up in an article entitled 'Towards a global law of electronic evidence? An exploratory essay'.[1]

As noted above, the aim is to help judges and lawyers to more fully understand the topic. I have two books on the subject: *International Electronic Evidence* and *Electronic Evidence*.[2] The University of London and the Institute of Advanced Legal Studies in London will shortly be initiating a web site where they will be hosting books that will be open source. I have agreed that the 4th edition of *Electronic Evidence* will go online for free in early 2017. The 4th edition of my book *Electronic Signatures in Law* will be the first legal book to be made available on this web site in the late autumn of 2016.[3]

II THE LAUNCH OF THE CONVENTION

The consultation on the Convention was launched at the DataFocus 2016 conference in Zagreb on 5 April 2016, and a Workshop on the Draft Convention on Electronic Evidence took place on 20 May 2016 between 14:30 and 17:00 at the Institute of Advanced Legal Studies in London. All of the information as set out on the Convention web site, and the details and names of the participants will appear as an annex to the Convention when it is published.

III THE DIFFERENCE A CONVENTION COULD MAKE

We have to think about electronic evidence in a different way to paper and other more familiar forms of evidence. In particular, we have to think about the authentication of electronic evidence and the need to encourage governments to permit the faster movement of evidence across jurisdictional

---

[1] Published jointly by *Amicus Curiae The Journal of the Society for Advanced Legal Studies* (2015) 103(Autumn), 19; and *Revista de Concorrência e Regulação* (2015) Ano VI, number 23-24 (julho–dezembro), 239.

[2] Stephen Mason (ed), *International Electronic Evidence* (British Institute of International and Comparative Law, 2008); Stephen Mason *Electronic Evidence* (LexisNexis Butterworths, 3rd ed, 2012).

[3] Stephen Mason, *Electronic Signatures in Law* (University of London, 4th ed, 2016).

boundaries. We live in a networked world, and it is important for judges and lawyers to understand the importance of the topic.

In the criminal context, Mutual Legal Assistance can be slow, and prosecuting authorities sometimes do not proceed with a possible prosecution because the evidence is not forthcoming from the requested state. Such a Convention might encourage a positive change. In this context, the most significant challenge is to ensure the text does not clash with national laws, and to draft in such a way as to encourage states to alter domestic law that helps with the admission and authentication of electronic evidence.

The consultation closes on the 30th September 2016. The final version will be published in the *Digital Evidence and Electronic Signature Law Review* in the autumn of 2016.[4]

[4] For more see, Convention on Electronic Evidence, *Home* <http://conventiononelectronic evidence.org>; Digital Evidence and Electronic Signature Law Review, *Home* <http://journals .sas.ac.uk/deeslr>; Stephen Mason ©.

Territorial Sovereignty in the Cyber Age

Angus Fraser*

I INTRODUCTION

While the internet is often utilised as a tool for greater connectivity and cooperation, the capacity to transmit information globally has created new threats for States.[1] The 21st century has heralded an increasing variety of malicious cyber activity, ranging from espionage to the destruction of physical infrastructure.[2] The most sophisticated of these attacks are State-sponsored.[3] The challenge for international law is to regulate the conduct of States by reconciling traditional concepts of Westphalian sovereignty with novel situations created by emergent technologies. The territorial boundaries separating States, which have existed since the inception of modern international law, appear anachronistic compared to cyber activities that can traverse those same boundaries with ease. As State-sponsored cyber activities continue to infringe upon the sovereign interests of other States, it is becoming increasingly pertinent to circumscribe the exact parameters of international law in cyberspace. Articulating prohibitive rules would demonstrate to States that their behaviour is not tolerated and their conduct may be subject to international adjudication.

The majority of scholarly efforts to address the lacunas in international cyberspace law have focused on the kind of high-intensity operations that have implications for the conduct of warfare. By contrast, there is a paucity of scholarship and jurisprudence that addresses low-intensity cyber operations that result in no or only minor damage. As a result, any statements as to their legal scope must rely on analogy with existing norms of international law. The prohibition on violating the territorial sovereignty of a State is a rule of international with a particularly low threshold to be breached comparative to other norms of international law. If the treatment of territorial sovereignty in existing international jurisprudence is analysed, there are basic elements applicable in a variety of different situations. Accordingly, there is no reason why the cyber realm should be exempt from the same kind of rules of

---

* BA/LLB candidate, TC Beirne School of Law, The University of Queensland..

[1] Centre of Excellence Defence Against Terrorism, *Responses to Cyber Terrorism* (IOS Press, 2008).

[2] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014) 6.

[3] Kim Zetter, *An Unprecedented Look at Stuxnet, The World's First Digital Weapon* (2014) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.

international law in relation to low-intensity cyber operations. Therefore, any conduct that involves the unauthorised interaction with cyber infrastructure in the territory of another State is a violation of its sovereignty and an internationally wrongful act.

II THE TALLINN MANUAL AND SOVEREIGNTY

The Tallinn Manual on the International Law Applicable to Cyber Warfare ('The Tallinn Manual') is the preeminent source describing the extant status of international cyber law. [4] The Tallinn Manual was the product of a three-year project by a group of twenty international experts on the topic of cyber operations.[5] It was commissioned by the North Atlantic Treaty Organisation Cooperative Cyber Defence Centre of Excellence.[6] The Tallinn Manual was initiated in response to distributed denial of service ('DDOS') attacks on critical service infrastructure in Estonia.[7] It is ironic, however, that the Tallinn Manual dedicates little attention to the kind of low intensity cyber operations that inspired its creation.

The Tallinn Manual adopts the widely held opinion that cyber attacks can qualify as a 'use of force' in international law.[8] In analysing whether a cyber operation constitutes a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the activity resembles that which would be considered a use of force if produced by traditional kinetic weapons. Legal Advisor for the United States Department of State Harold Koh has identified common examples of cyber activity that would constitute a use of force. Examples include operations that trigger a nuclear plant meltdown, opening a dam above a populated area causing destruction, or disabling air traffic control resulting in aeroplane crashes.[9] All of the scenarios have a tangible quality that makes accepting their illegality a more palatable proposition than cyber espionage or DDOS attacks, which may not result in easily quantifiable harm.

However, it is exactly those kind of activities that are both the most common and least regulated cyber operations. On the topic of sovereignty, the Tallinn

---

[4] Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Tallinn Manual* (2016) <https://ccdcoe.org/research.html>.
[5] Michael Schmitt, 'The Law of Cyber Warfare: *Quo Vadis*?' (2014) 25 *Stanford Law and Policy Review* 269, 270.
[6] Zetter, above n 3.
[7] CCDCOE, above n 4.
[8] Ibid 42-52.
[9] Harold Koh, *International Law in Cyberspace*, speech delivered on 18 September 2012 at the USCYBERCOM Inter-Agency Legal Conference, Fort Mead, Maryland.

Manual states that 'a State's sovereignty over cyber infrastructure within its territory has two consequences. First, that cyber infrastructure is subject to legal and regulatory control by the State. Second, the State's territorial sovereignty protects such cyber infrastructure. It does not matter whether it belongs to the government or to private entities or individuals, nor do the purposes it serves matter.'[10] The Tallinn Manual defines cyber infrastructure as 'the communications, storage, and computing resources upon which information systems operate.'[11] It further states that there was no consensus amongst the experts as to whether a violation of territorial sovereignty will have occurred with respect to cyber attacks causing no physical damage.[12]

Physical damage appears to be an arbitrary qualifier in practice, considering the massive financial or strategic loss that can result from cyber attacks. For instance, data breaches in the United States have included the mass collection of personal data belonging to over 21.5 million individuals from the Office of Personnel Management last year.[13] Millions of dollars are lost annually in cyber espionage activities that acquire sensitive intellectual property.[14] In fact, a Chinese businessman was recently arrested for conspiring with the Chinese People's Liberation Army to acquire American military secrets.[15] But the domestic legal framework that criminalises the conduct of individual actors has thus far avoided translation into norms outlawing States from engaging in the same operations.[16] It is critical that international law keeps pace with the manner in which novel technologies can compromise the essential interests of States. The inherent difficulty of establishing a legal prohibition on such activities is the fact that some States benefit from an ostensible 'grey area' in international law.[17] For these States the cost of being subject to data breaches may be an acceptable loss if they can benefit from their own unregulated conduct. But for many other States, there is little they can do to prevent cyber attacks and even less they can do receive legal recourse.

---

[10] International Group of Experts, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) 15-16.
[11] CCDCOE, above n 4, 278.
[12] Von Heinegg (2013), 129; CCDCOE, above n 4, 16.
[13] OPM, *Cybersecurity Resource Centre* (2016) <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>.
[14] Catherine Lotrionte, 'Countering State-Sponsored Cyber Economic Espionage Under International Law' (2015) 40 *North Carolina Journal of International Law and Commercial Regulation* 443.
[15] BBC News, *US Sentences Chinese Hacker for Stealing Military Information* (2016) <http://www.bbc.co.uk/news/world-us-canada-36791114>.
[16] Matthew Sklerov, 'Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent' (2009) 201 *Military Law Review* 1, 9-10.
[17] Tyra Saechao, 'Natural Disasters and the Responsibility to Protect: From Chaos to Clarity' (2007) 32 *Brooklyn Journal of International Law* 663, 681.

III TERRITORIAL SOVEREIGNTY IN INTERNATIONAL LAW GENERALLY

The basic principle of the sovereign equality of States is articulated in Article 2(1) of the 1945 *Charter of the United Nations*.[18] However, the specific rule prohibiting the violation of another State's sovereignty was first considered by the International Court of Justice ('ICJ') in the 1949 *Corfu Channel* decision.[19] The proceedings concerned two incidents involving the entry of British warships into Albanian territorial waters. The Court held that the entry of warships without consent was a violation of Albania's sovereignty.[20]

In 1960 the Soviet Union raised the issue of violated sovereignty before the United Nations Security Council. The complaint concerned what is known as the U-2 incident: the capture of US pilot Garry Powers after he crashed a spy-plane in Soviet territory.[21] While it was not subject to any kind of judicial consideration, the incident is an early demonstration of *opinio juris* that the territorial airspace of a State may not be violated by another for the purpose of espionage. Pertinently, the US did not seek to argue that its action was legal. Instead, it sought to justify its actions on the unpersuasive basis that reconnaissance was a necessary evil in order to prevent greater conflict during the Cold War.[22]

The concept of territorial sovereignty was subsequently raised in the Nuclear Tests Cases between France, Australia and New Zealand.[23] The applicant States argued that nuclear material from tests conducted by France in the South Pacific between 1966 to 1972 had entered their territory without consent.[24] The cases did not proceed to consideration on the merits because France made a declaration that it would cease testing.[25] The acuity of the submissions concerning sovereignty was therefore never assessed by the majority of the Court.

---

[18] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14, 212.
[19] *Corfu Channel (United Kingdom v Albania) (Merits)* [1949] ICJ Rep 4 ('*Corfu Channel*').
[20] Ibid 36.
[21] *Verbatim Record of Meeting*, UN SCOR, 860th mtg, UN Doc S/PV.860 (26 May 1960) 1-3.
[22] Ibid.
[23] *Nuclear Tests case* (*New Zealand v France*) [1995] ICJ Rep 288, 378.
[24] *Request for the Indication of Provisional Measures of Protection Submitted by the Government of Australia* [1973] ICJ Rep 43.
[25] *Nuclear Tests case* (*New Zealand v France*) [1995] ICJ 288.

Writing in 1983, Ian Brownlie posited that there is a cause of action in international law that States may not violate one another's sovereignty.[26] He successfully argued this in the 1986 *Nicaragua v US* case before the ICJ. The court accepted that the unauthorised entry of surveillance aircraft into Nicaragua's territory to conduct reconnaissance overflights and perform sonic booms were violations of sovereignty.[27] It considered the laying of mines in Nicaragua's territorial waters to be a similar violation, but also a use of force.[28] Because of the nature of the Court's jurisdiction in that case, the ICJ could only relevantly consider customary international law.[29] The violation of a state's territorial waters or airspace under treaty law was therefore not considered. In that same year an arbitration occurred between New Zealand and France over the sinking of the *Rainbow Warrior* vessel in New Zealand by French agents.[30] The arbitrator, UN Secretary-General Javier Pérez de Cuéllar, considered the acts of those agents on New Zealand territory to be a violation of its sovereignty.[31]

Subsequent judgements have dispelled any doubt that the ICJ was concerned in previous cases only with specific regimes that prohibit violations of territorial waters or airspace. The *Armed Activities* decision in 2005 concerned the breach of the tripartite agreement between The Democratic Republic of Congo, Rwanda and Uganda.[32] Even thought the Court was primarily concerned with treaty breach, the majority noted that 'an obligation in an international agreement to respect the sovereignty and territorial integrity of the other States parties to that agreement … exists also under general international law.'[33] In December 2015 the ICJ made a decision on two matters that had been joined. The case concerning *Certain Activities Carried Out by Nicaragua in the Border Area and Construction of a Road in Costa Rica* was, inter alia, about the presence of Nicaraguan troops and dredging in a disputed territory.[34] Once the court decided that the territory belonged to Costa Rica it held that, ipso facto, Nicaragua had violated Costa Rica's territory through conduct of

---

[26] Sir Ian Brownlie, *System of the Law of Nations, State Responsibility (Part I)* (Oxford University Press, 1983).
[27] *Nicaragua v United States of America*, 147 [5].
[28] Ibid 6.
[29] Ibid 43.
[30] *Rainbow Warrior (New Zealand v France)* (1990) 20 UNRIAA 217 ('*Rainbow Warrior*').
[31] Ibid 271.
[32] *Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda) (Judgment)* [2005] ICJ Rep 168, 255 [256] ('*Armed Activities*').
[33] *Armed Activities* [2005] ICJ Rep 168, 256 [257].
[34] *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica (Nicaragua v Costa Rica) (Judgment)* (International Court of Justice, General List No 150 and 152, 16 December 2015).

activities there without its consent.[35] The case is important in two respects. Foremost, it further entrenches a clear attitude by the Court that a violation of sovereignty is in fact a separate wrong under international law, and not simply an umbrella term that encompasses more specific wrongs such as a violation of airspace. Secondly, it affirms that the *activities* of organs in a territory is a violation of its sovereignty and not simply the fact that they entered without permission. In this sense, the wrong is not limited to the disrespect of a State's border, but also the infringement on the right of a State 'to exercise to the exclusion of any other State, the functions of a State'[36] on its territory. The activities in question were of particularly low intensity, as the Court made reference to the dredging of the San Juan river in the orders of its judgment.[37]

The decision necessarily raises a question as to what kind of limit is placed on conduct by a state within another's territory. Is there a *de minimis* threshold that must be overcome before the act in question is considered internationally unlawful? Or is any unauthorised activity sufficient to constitute a violation? An affirmative answer to the latter question is best understood as premised not in the harm caused but in the lack of respect for the exclusive jurisdiction of the affected State. Interference within the territory of another State is therefore effectively a usurpation of jurisdiction. The ICJ has not required the occurrence of physical damage as a predicate to violating sovereignty in any of its previous judgments. By contrast, the Court's approach to environmental transboundary harm has been to outline a lower limit on what kind of activities would enliven state responsibility. The 1941 *Trail Smelter Arbitration* and 2010 *Pulp Mills* decision both considered that only *significant damage* would be a violation of the respective treaties in those cases prohibiting transboundary pollution.[38] The International Law Commission's *Draft Articles on Transboundary Harm*, while generally pronouncing on the nature and scope of due diligence, nevertheless adopt the language of significant harm.[39] The difference between transboundary harm and the aforementioned examples of violated sovereignty is that the former is premised in due diligence. Due diligence entails an omission on behalf of agents of the State to exercise best efforts or due care in

---

[35] Ibid 48 [113].
[36] *Island of Palmas (Netherlands v United States of America) (Award)* [1928] 2 RIAA 829, 838.
[37] *Costa Rica v Nicaragua*, 229 (2).
[38] *United States of America v Canada* (Award, Trail Smelter Arbitration, 16 April 1938 and 11 March 1941) (1941) 3 RIAA 1905, 1965; *Pulp Mills on the River Uruguay (Argentina v Uruguay) (Judgment)* [2010] ICJ Rep 14, 101.
[39] International Law Commission, 'Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with Commentaries' [2001] II (2) *Yearbook of the International Law Commission* 148.

their conduct.[40] By contrast, where a State knowingly and deliberately commits activity in the territory of another without permission, there is an explicit disregard for the sovereignty of the other State.

IV VIOLATIONS OF SOVEREIGNTY IN A CYBER CONTEXT

Cyber-space is considered by some commentators to be a global, unregulated common.[41] However, the attitude of States as evidenced by their domestic policies and numerous international instruments does not support this proposition.[42] For instance, the United Nations Institute for Disarmament Research indicates that at least 32 States have included cyber warfare in their military planning and organisation.[43] The Wales Summit Declaration issued by the North Atlantic Council member heads of State and government recognises that '…international law, including international humanitarian law and the UN Charter, applies in cyberspace.'[44] As the 2011 US International Strategy for Cyber-space states, 'long-standing international norms guiding State behavior in times of peace and conflict also apply in cyber-space.'[45] While a suppression instrument, the Council of Europe Convention on Cybercrime is also evidence of an attitude by States that cyberspace is legally regulated.[46] The bridge between the cyber realm and the tangible is the underlying infrastructure that

---

[40] Pierre-Marie Dupuy, 'Reviewing the Difficulties of Codification: On Ago's Classification of Obligations of Means and Obligations of Result in Relation to State Responsibility' (1999) 10(2) *European Journal of International Law* 371.

[41] Michael Schmitt 'The International Law of Attribution During Proxy "Wars" in Cyber-space' (2014) 1 *Fletcher Security Review* 4.

[42] Eneken Tikk, 'Ten Rules for Cyber Security' (2011) 53(3) *Survival* 119; *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN GAOR, 68th sess, Agenda Item 94, UN Doc A/68/98 (24 June 2013) [27], [28](b); United States of America, Department of Defence, 'The Department of Defence Cyber Strategy' (White Paper, April 2015) < http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>, 9; United Kingdom, Cabinet Office and National security and intelligence, 'Cyber Security Strategy' (2011) <https://www.gov.uk/government/publications/cyber-security-strategy> 27; People's Republic of China, The State Council Information Office, 'China's Military Strategy: IV Building and Development of China's Armed Forces' (White Paper, May 2015) <http://eng.mod.gov.cn/Database/WhitePapers>; Japan, Ministry of Defence, 'Defence of Japan: Section 5, Trends in Cyber-space' (White Paper, 2015) <http://www.mod.go.jp/e/publ/w_paper/2015.html >.

[43] UNIDIR/2013/3.

[44] NATO, *Wales Summit Declaration*, 2014 <http://www.nato.int/cps/en/natohq/official_texts_112964.htm> [72].

[45] United States of America, Department of Defence, 'International Strategy For Cyber-space' (May 2011) *<https://www.whitehouse.gov/sites/default/.../international_strategy_for_cyber-space.pdf> 9.*

[46] *Convention on Cybercrime*, ETS 185 (entered into force 23 November 2001).

supports computer networks. For example, servers are physical computer infrastructure that may be located in the territory and jurisdiction of a State.[47]

As discussed, under international law the conduct of activities without consent in the territory of another State is a wrong, not simply the unauthorised crossing of that State's border.[48] This is particularly important in the cyber context where the actual crossing of a State's border by electronic data is difficult to analogise with physical traversal. If the position is adopted that any unauthorised activity whatsoever (with or without the advent of physical damage) is a breach of international law, the kinds of activities that would be internationally unlawful is admittedly broad. Conducting cyber espionage in another state's territory is a violation of their sovereignty.[49] Purely disrupting the software of computer systems is, in the absence of consent, a violation of sovereignty.[50]

However, if it is well established that using a plane to spy on another State is a violation of its sovereignty, then spying done in a more clandestine manner must surely not be more permissible because it involved no physical presence. This would contradict the concept that international law seeks to avoid situations of *non liquet*.[51] In fact, permitting low-intensity cyber operations is in contravention of the most basic principle enunciated by the Permanent Court of International Justice in the 1927 *Lotus Case*.[52] The precursor to the ICJ held that States are free to do anything not prohibited by international law, as long as it does not interfere with the exclusive jurisdiction of another State.[53] This principle has been progressively eroded by treaties and concepts such as humanitarian intervention, but at its core it remains a relevant proposition. Simply put, unless there is a customary *exception* to this general rule, States may not interfere with one's another's sovereignty by conducting activities in each other's territories without consent. There is insufficient State practice and *opinio juris* to suggest that such an exception exists. While States may anecdotally conduct invasive cyber operations like espionage, in order for there to be an exception, general and consistent state practice is required.[54] Their

---

[47] Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyber-space' (2013) 89 *International Law Studies* 123, 140.
[48] *Costa Rica v Nicaragua*, 48 [113].
[49] Antonio Cassese, *International Law* (Oxford University Press, 2nd ed, 2005), 51-2.
[50] Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyber-space' (2013) 89 *International Law Studies* 123, 128-9.
[51] Prosper Weil, '"The Court Cannot Conclude Definitively ..." Non Liquet Revisited' (1997) 36 *Columbia Journal of Transnational Law* 109.
[52] *SS 'Lotus' (France v Turkey)* [1927] PCIJ (Ser A) No 10 ('*Lotus Case*').
[53] Ibid 18.
[54] *Nicaragua v United States of America,* [186].

reticence to acknowledge responsibility for these actions may also suggest that that the conduct is considered to be unlawful by the international community.

There are also countervailing factors that reduce the likelihood of States successfully challenging every instance of cyber intrusion in a 'floodgates' style scenario. Even if the bar to violating international law is low, the attribution for cyber crime or cyber attacks is necessarily difficult. An applicant State must establish that the perpetrators behind an attack were the organs of another State in accordance with its internal law, empowered by the law of the State as functionaries, or under the effective control of the State.[55] Unsurprisingly, Foreign Ministers frequently deny official involvement in cyber attacks when accused.[56]

Proving that one of these categories of agents actually committed an act is extremely difficult, largely due to evidentiary issues. The standard adopted by the ICJ in such a situation is beyond a reasonable doubt or 'fully conclusive.[57] Former president of the ICJ Dame Rosalin Higgins has stated that the two standards are comparable.[58] With the exception of direct evidence such as a witness statement or footage of State agents launching a cyber attack, is it difficult for a State to establish that another launched a cyber attack of any nature, be it high or low intensity.[59]

There is a further practical limitation on a broad definition of low intensity cyber operations. Simply put, States may be reticent to proceed through the ardour and cost of going to the ICJ over simple matters. Just because a State *can* proceed to the Court doesn't mean it will. Moreover, the Court has been content to merely make a declaration of a violation of international law as appropriate satisfaction, such as in *Corfu Channel*.[60] Therefore, there is no guarantee that, even if a State has violated another's territorial sovereignty, it will have to compensate the victim State if the violation was insignificant. But

---

[55] International Law Commission, 'Report of the International Law Commission on the Work of Its Fifty-Third Session (23 April - 1 June and 2 July - 10 August 2001' [2001] II (2) *Yearbook of the International Law Commission* 31, arts 4, 5, 8.

[56] Eg Lizzie Dearden, *US government hack: China denies responsibility for cyber attacks that stole personal details of four million employees* (2015) <http://www.independent.co.uk/news/world/americas/us-government-hack-live-china-denies-responsibility-for-cyber-attack-that-stole-personal-details-of-10298745.html>; Xinhua, *Iran denies involvement in cyber attacks on U.S. Institutions* (2016) <http://news.xinhuanet.com/english/2016-03/26/c_135225830.htm>.

[57] *Corfu Channel,* 18; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 43, 129 [209].

[58] Rosalyn Higgins, *Speech by H.E. Judge Rosalyn Higgins President of the International Court of Justice to the Sixth Committee of the General Assembly* (2 November 2007) 5.

[59] *Oil Platforms (United States v Iran)* [2003] ICJ Rep 161.

[60] *Corfu Channel,* 36.

what is most important is that there exists a legal framework that prohibits and disincentives violations of sovereignty that States would be otherwise powerless to prevent. The significance of an intrusion should be decided by the ICJ, not by an arbitrary limitation that limits justiciable cases to only those involving physical damage.

V CONCLUSION

The ICJ has articulated a consistent rule of international law, from its very first case, that a State may not violate the sovereignty of another. This occurs through the conduct of actions by one State in another's territory without the latter's consent. The ICJ has not limited the rule to specific areas of a State's territory. Nor has it articulated a minimum threshold of damage that must be overcome in order to qualify as a violation of territorial sovereignty. Accordingly, there is no reason why sovereignty may not be violated through a cyber medium, provided that the computer infrastructure directly affected is within the territory of a State and its exclusive jurisdiction. While the Tallinn Manual reports a lack of consensus on the correctness of this position, the jurisprudence of the ICJ firmly supports it. With the release of Tallinn 2.0 expected this year,[61] it is hoped that the group of experts takes the position in favour of preserving the integrity of States over an arbitrary requirement that physical damage must occur for there to be a violation of international law. A statement to the contrary would be a disservice to the continued efficacy of international law in the 21st century.

[61] Michael Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 *Yale Law Journal* 68.

Pandora's Box
2016 *Law and Technology*

A publication of the Justice and the Law Society
THE UNIVERSITY OF QUEENSLAND

ISSN - 1835-8624