Cloud Computing Regulation: An Attempt to Protect Personal Data Transmission to Cross-Border Cloud Computing Storage Services

Abdallah AbuOliem

***Abstract*—Cloud computing has become popular for its users who need low-cost and large scale computing. Lately, international and regional organizations as well as governments have begun to understand the legal impact of cross border cloud computing storage service on individuals' personal data. To meet the need of personal data protection regulations, this study discusses the significance of personal data protection. In addition, personal data protection in the current use of a specific storage characteristic in cross border cloud computing. The threats associated with the cross border transmission of personal data. This study describes the level of understanding the risk of business departments and governments' agencies that implement this technology. Furthermore, this study examines the variety of alternative jurisdictions existing around the world. Based on an examination of these jurisdictions and the benefits that accrue through the adoption of regulatory framework, this study argues that defined elements for protection of personal data transmitted to cross border cloud computing technology are an essential part of any future attempt to cloud computing regulation.**

***Index Terms*—Cloud computing regulation, cross border cloud computing risk, personal data transmission, cloud practice, personal data protection.**

I. Introduction

Cloud computing, which permits for highly accessible computing applications, storage, and platforms, is growing in importance throughout the field of regulation information technology (IT) [1]. Cloud computing providers make available a variety of services to individuals, companies, and government agencies, with users engaging in cloud computing for storing and sharing information, database management and mining, and deploying web services, which can change from processing huge datasets for difficult scientific problems to using clouds to accomplish and deliver access to medical records [2]. The USA President Barack Obama and the US Chief Technology Officer Vivek Kundra have both acknowledged the vision to discover the cloud as an essential part in the federal program of information technology renewal, and therefore agency use of cloud computing capabilities has increased [3].

The increase of cloud computing practice [4] has led individuals to be cautious in relation to knowing where their personal data is stored; who sees it, who ensures it is correct, etc. [5]. Furthermore, individuals may demand the right to control their personal data [6]. As many technologies related to the internet have a real influence on excess of personal data, the importance of creating trust and confidence can lead to better internet practices and economic growth [7]. Many cloud computing providers have expressed their opinion on the protection of individual's personal data. For example, Google's chief executive Eric Schmidt echoed such sentiment when he said, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"[8]. A month before Schmidts comments, Facebook's founder and Chief Executive Mark Zuckerberg declared "the age of privacy to be over" [9]. It is a huge concern for everyone who believes in personal data protection when the two bosses from the biggest personal data storage companies in the world claim that personal data, which they do not own in the first place, is not respected anymore. Their views also raise concerns because it simply shows their relaxed personal view in protecting the personal data of billions of users. Governmental bodies around the world are now recognising the significance and urgent need for establishing regulations in relation to cloud computing [10]. For example, the recommendation made by the Congress of the Liberal Democratic Party to the British Government in September 2011, concerning the adoption of cross border cloud computing in England [11] reads: "We have noted the growing popularity of cloud computing. It is clear that this new technology provides tremendous opportunities to streamline the use of IT, reducing costs and driving up efficiency.

However, cloud computing is an area where, if left unchecked, there is serious potential for abuse.

Cloud Computing is only attractive if it embodies the principles on privacy and data ownership, access, project management and procurement.

We recommend that as a matter of urgency, the government consider the security issues involved with cloud computing, particularly regarding data location and segregation".

Although cloud computing can provide many benefits, there are also many legal obstacles and challenges associated with adopting cloud computing technology [12]. The adoption may compromise the rights to personal data due to jurisdiction control of personal data. According to Foster, Zhao, Raicu, and Lu, the new personal data protection threats are privileged user access, long term viability, data segregation, recovery, investigative support, data location and applicable law [13].

As the focus of this study is on cross border cloud computing risks, this paper argues that laws and standards

Manuscript received January 15, 2013; revised April 15, 2013.

Abdallah AbuOliem is with the Department of Accounting & Corporate Governance, Faculty of Business & Economics, Macquarie University, Sydney, Australia (e-mail: Abdallah.abuoliem@mq.edu.au).

can be designed by each country's' local data protection law such as the United Kingdom (UK), Australia and the United State of America (USA) or by particular region regulation such as European Union (EU) and Asia Pacific Economic Co-operation (APEC) or by international standard such as Organisation for Economic and Co-operation Development (OECD). Any personal data collection services (data controller) that use cross boarder cloud computing storage services should be aware that the jurisdictions where data centers are located and the laws that may be applicable [14]. This requires high level understanding and management before the personal data can be transfer to cloud computing provides located in other jurisdictions. Hence, cross boarder data storage is one of the key clouds computing legal issue which may cause loss of control to individuals' personal data by shifting the applicable law to another jurisdiction.

II. Back Ground

Cloud computing technology has experience a high reputation among their users and advanced faster than the regulation can adapt to it [15]. This often can be understood in the early stage of services growth. Hence, Stylianou examines the factual implication of this new concept called cloud computing services. He found some ambiguity on how the new services should be regulated as cloud computing leads to come new opportunities and new risks [15]. Soma, J. et al, believe that personal data issue is critical component to the successful adoption of cloud technology and the need to avoid the inherited risk of. They demonstrate how it is the right time to take an action toward cloud computing regulation [16]. Stylianou claims that there is no doubt that some legal gaps still exist [15]. Despite the fact that some of these gaps are filled in by contractual terms, but these terms are not always fair or clear. To protect personal data transmission to cross-border cloud computing storage services, the regulatory framework provisions need to be transparent, effective and geared towards protecting the rights to personal data.

King and Raja analyses the effectiveness of the current legal framework in Europe and the USA in relation to the protection of sensitive personal data in the cloud. They come to a conclusion that regulatory reform is needed to protect personal data in the cloud computing environments and delete sections that constrain the growth of the cloud industry [17]. In addition, Robison noted that the courts will face their most difficult task in determining how cloud computing suits within the Stored Communications Act (SCA) complex framework. He claims an old fashion twenty years old SCA, a component of the broader Electronic Communications Privacy Act (ECPA), is the primary federal source of online personal data protection [18].

III. Research Aims and Objectives

A. Aims

The aims of this paper are to highlight the absence of a legal framework for governing personal data transmission to cross border cloud computing services and explore the benefits that may accrue through the adoption of essential elements in the regulatory framework. Moreover, this study examines the variety of alternative models in existence around the world. Based on an examination of these models and cloud computing own unique features, this study seeks a regulatory framework for the protection of personal data in relation to cloud computing.

B. Objectives

The objectives to be achieved in this study though the following:

1) To define the concept of personal data in order to develop a working definition of personal data. Highlights the importance rights of personal data and it reviews the current recognition and standard.
2) To investigate the situation regarding personal data protection and cloud computing. It is essential to evaluate to what extent personal data is protected in cloud computing that is used by many sectors.
3) To identify threats to personal data transmission to cloud computing service provider and reveal to what extent current practices trespass individual personal data.
4) To identify the suitability of the current international models of personal data protection. This will be necessary to discover the different proposal and approaches that are attempting to govern "cloud computing". It evaluates the OCED as international standard approach and the Directive 95/46/EC and APEC as regional approach and then the UK as single national regime. Finally, to recognize exemption, applicable law, enforcement mechanism and remedies to personal data protection.
5) To determine the essential elements in the regulatory framework for the protection of personal data in cross border cloud computing storage service.

IV. Research Importance

A. Significant of the Research

Having confidence is one of the core factors influencing user adoption of cloud services, [19]. User adoption should not only be a paper- based exercise at any point but it also needs to be transparent, effective and not compromise the right to personal data as primary components. As outsourcing cloud computing storage service is growing rapidly [20], a practical and sensible regulatory approach to protect personal data transmission in information technology environment is of paramount importance [21].

It is essential to balance the threat of transmission between users and cross-border cloud service providers and ensure that services are aligned with regulatory elements to ensure protection of users' personal data [22]. Hence, cross border cloud computing provider should be working to implement the essential elements in the regulatory framework to meet their legal requirements [23].

B. Significance to Law Makers (Regulators)

Regulators need to take into consideration all three elements in order to a) understand what are the regulatory elements to be employed at the present and in the future, to

meet cloud computing specific characteristic [24] b) understand who owns the personal data, what rights exist in relation to personal data and what it means to cloud service providers [25] d) going beyond the traditional national border mind in designing law to cover multinational approach and focusing on mitigating a predictable law and enforcement mechanism [26]. This is important implication for regulators as we have seen several times already how loss of confidence after data leakage can be serious problem for individuals [27]. During the last years, the concept of cloud computing has been taken up by many international organizations such as OCED Guideline and APEC Framework on cross border transmission of personal data. Therefore, the space and degree of cloud computing responsibility was broaden and should be adapted to the fresh needs of the overall society [28]. Furthermore, the European Union (EU) has become active by submitting a new Data Protection Directive (DPD) proposal [29] in order to support the current softening legal approach. [30].

C. Significance to Cloud Computing Industry

Do cloud computing service providers have a responsibility to society [31]? The responsibility exceeds more than legal obligations and includes the integration of social, ethical and human rights as well as users concerns into the operation comply with the society's expectations of personal data protection [32]. This means to have a (risk-based due diligence) process in place which interconnect consistency in contract terms and condition with any applicable cloud computing regulatory framework and prevent any negative legal impact on their business [27].

Cloud computing providers based in US appear not to be liable for direct responsibility as far as fines are concerned. On the other hand, European based cloud providers remained less open about looking for exclusion of direct responsibility because it is difficult to do so in most European legal systems. The restriction in both jurisdictions may be an important factor for individuals to anticipate in their selection of cloud provider. This also highlights the fact that complete abdication of responsibility may not be enough to local state regulations. In the UK for example, individuals sensing cloud computing agreement terms are unfair and may have some remedy under the Unfair Terms in Consumer Contracts Regulations [33]. For example, in Amazon web services term of use, state that "we strive to keep your content but cannot guarantee that we will be successful at doing so, given the nature of the internet".

Cloud computing obligations are not a totally new concern but it was arguing in a normative way that it refers to the obligation of cloud computing provider to pursue untied regulations in order to make those decisions which are not desirable in terms of protecting human rights and the value of society [34]. As Tim Watson, head of the computer forensics and security group at De Montfort University, points out that there are some providers that may offer a delightful protection of personal data and another may not. If the ones who do not provide sufficient service charge only half price for example, the majority of users will go with it as they do not really have a means of judging the differences apart from the price. Hence, when time passes by and as publicity over personal data protection breach continues to grow, the entire cloud computing sector may not be trustworthy and then the industry would be destroyed [35].

V. Motivation and Expected Contributions to Body of Knowledge

The motivation for this study is maximizing the control of individual personal data transmission to cloud computing services in another jurisdiction. The risk facing regulators of moving data into a cross border cloud computing field were recognized as the main investigation area of this study. As a result of cross border risk, a considerable number of financial institution and governments departments hesitate to adopt cross border cloud technology. Therefore, the need of increasing confident in cross border cloud computing by providing regulatory protection solution.

In addition, the expected contribution to the body of knowledge is to provide the essential regulatory elements and void any negative jurisdictional impacts of the cross border cloud computing on individual personal data. It will clear that the important legal information that needs to be known before transmission of personal data to cross border cloud computing is the legal norms in the target jurisdiction. Furthermore, it covers a broad literature review on the transmission of personal data laws relating to the Information and Communication Technology (ICT) as related to cross border cloud computing. The recognition of personal data rights in the international and national jurisdictions will be inspected. Features around the cloud were also examined in order to understand what feature would be appropriate to address the personal data protection issue. Abroad exploration of regulations on data protection also expected to find the elements for any future cross border cloud computing regulations.

VI. Research Scope and Limitations

This study is to establish the elements of personal data provisions in relation to the emerging cross border cloud computing technology. The study is intended for cloud computing providers and regulators who intend to establish the criteria for personal data protection from cross border risks. The study does not touch or resolve a final classification of cloud computing. Nor does it try to be an exhaustive study on cloud architecture and design. Although cloud computing phenomena is still at its initial stage with much more research to come, it is the correct time for laws, standards and policy makers of the merging cloud computing to come together around the idea of appropriate regulatory framework in protecting personal data transmission to cross border cloud computing storage service.

This paper urges cloud computing community to act soon to unite, modify and enhance the current framework to eliminate confusion of provisions applies to a cross border cloud computing storage service. It advocates for clarify clarification of the boundaries of personal data used in cross border cloud computing. It also helps in establishing a right to personal data in the cloud computing space. Finally, this study discusses the cross jurisdictional question. Since the

study is limited by content, length and time, it will be difficult to provide explanations to all the legal subjects touching cloud computing. Nor will it be promising to determine more than six different jurisdictions dealing with personal data transmission to cross border cloud computing.

VII. Future Work and Research

The author's observation of the literature shows current gaps in the existing literature in association with cloud computing regulation. Today the unknown impact of cloud implication on business developments, organization dynamic, price saving and income generation will grow in significance as cloud transfer continues to develop and touch ordinary status in businesses. Nowadays, there is a current need for research that underpins the stage and offers a platform from which other can construct. It is the time for studies that identify best standard practices, critical success elements, and other implementation issues. In addition to studies examining measured configuration and influence on business operations and work flow will be researchable.

As the legal debates increase and customer disputes are judged, more examples will appear. There are a number of cases being processed in courts. This would deliver a better insight into how courts will deal with cloud computing cases [18], [36], [37]. Cases are vary from civil disputes with cloud provides over to criminal charges for misbehavior. The new regulatory framework elements should help court in constructing decision on this merging technology.

VIII. Research Methodology

A. Methodological Path

In the search for a sufficient methodology for this study, the author previously wondered whether there is a formal research methodology in law. It has been noted that the methods that work in the legal scholarship are neither intentionally learned nor intentionally employed as in the case of scientific methods [38]. The uncertainty of formal methodology stems from the nature of legal scholarship that is based mostly on narrative and qualitative analysis rather than data collection and quantitative studies [38].

Becher (1987) has described 'knowledge production in the sciences in terms of the cumulative and piecemeal accumulation of individual segments of knowledge which, over time, contributes to a comprehensive explanation of particular phenomena' [38].

Relatively, this study follows the methodological path in line with Becher's description. This study keeps collecting the materials that establish whether personal data is human right or property right and constitute the conceptualisation of the right to personal data in 'cloud computing'. To accomplish this, it builds upon various body of knowledge and identifies the fine line between personal data protection and other concept such as freedom of expression.

The study attempts to develop a 'holistic understanding' and a well-rounded vision of the philosophical, ethical and normative aspect of the merging legal norm identified herein as personal data right in cross border cloud computing storage service. Based on Clare Cappa model for integration of legal research, the study falls into the theoretical research category which 'fosters a more complete understanding of the conceptual bases of legal principles and of the combined effects of a range of rules and procedures that touch on a particular area of activity' [39].

B. Forms of Investigation

The research will be pursued by a combination of the following forms of investigation:

1) The first level of analysis deals with the philosophical, ethical and theoretical underpinnings of the linkage between human right and personal data. To establish such linkages the study examines human relationship and the various ethical perspectives that originate from such philosophical debates and then reviews the theoretical foundation of right to personal data rights. Particular significance to this level of analysis is the notions of human dignity, and the universality and the individualistic nature of the human right.
2) Study needs also to describe both the existing law and the lack of law in current selective jurisdictions practice before it goes to the second level of analysis. The description part provides the operational dimension of the study to look into international, regional and national legislations. This dimension also contributes to the debate over which law and enforcement mechanisms are applicable.
3) The study examines a wide range of primary sources of laws and court cases and gathers comprehensive literature of relevant to the discipline. It is worth noting that the legislation and cases are carefully chosen base on their contribution towards regulatory framework elements
4) The second level of analysis attempts to construct the normative and legal models to personal data associated with cloud computing. It identifies and summaries the data protection laws provisions applicable to cross border cloud computing services. So far, there have been no complete regulation directly referring to cross border cloud computing.

C. Justifications

The domestic and international models are influential in interpreting the scope and content of personal data provisions governing cross border cloud computing services. The justification behind the broad coverage of existing models come from (1) the nature of international transmission of personal data to cross border cloud computing which is connected to its domestic counterpart through the internet (2) The violation of personal data rights can happen within domestic level or within the international level when authorities protection fail to guarantee these rights or to provide appropriate remedies.

IX. Conclusion

The legal effects of storing and moving personal data within a cloud computing atmosphere are uncertain. Regulations control the process of personal data transmission within countries. The potential location of cloud computing in various jurisdictions to supply the cloud

service appears to challenge the level of protection of personal data stored in cross border cloud computing and effect the mind that drafting and designing legislation. This study, via a literature review, has endeavored to comprehend the relevant legal issues regarding personal data in the field of cloud computing. The regulatory framework in relation to the protection of personal data transmission to cross border cloud computing ought to be employed in order to extract and integrate relevant perspectives into the legal questions facing cloud computing regulation.

REFERENCE

[1] S. S. Islam, M. B. Mollah, M. Huq, and M. Ullah, "Cloud computing for future generation of computing technology," in *Proc. IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems* (CYBER), 2012, pp. 129-134.

[2] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly*, vol. 27, no. 3, pp. 245-253, 2010.

[3] K. Irion, "Government cloud computing and national data sovereignty," *Policy and Internet*, vol. 4, no. 3-4, pp. 40-71, 2012.

[4] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?" *Journal of Information Technology and Politics*, vol. 5, no. 3, pp. 269-283, 2008.

[5] R. R. Arnesen, J. Danielsson, and N. Regnesentral, "A framework for enforcement of privacy policies," in *Nordic Security Workshop*, 2003.

[6] R. A. Spinello, "Privacy rights in the information economy," *Business Ethics Quarterly*, vol. 8, no. 4, pp. 723-742, 1998.

[7] C. F. Carlton, "The right to privacy in internet commerce: a call for new federal guidelines and the creation of an independent privacy commission," *Journal of Civil Rights and Economic Development*, vol. 16, no. 2, pp. 7, 2012.

[8] J. Grimmelmann, "Privacy as product safety," *Widener Law Journal*, vol. 19, pp. 793, 2010.

[9] B. Schneier, "Schneier on security: privacy and control," *Journal of Privacy and Confidentiality*, vol. 2, no. 1, pp. 2, 2010.

[10] J. Cave, N. Robinson, S. Kobzar, and R. Schindler, "Regulating the cloud: more, less or different regulation and competing agendas," TPRC, March 30, 2012.

[11] A. Guess.(July 2012). UK government called to examine security of public data in the cloud data versity. [Online]. Available: http://www.dataversity.net/uk government-called-to-examine-security-of-public-data-in-the-cloud/

[12] D. Catteddu, "Cloud computing: benefits, risks and recommendations for information security," *Web Application Security*, vol. 72, pp. 17, 2010.

[13] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Proc. Grid Computing Environments Workshop, IEEE*, 2008, pp. 1-10.

[14] J. Bing, "Data protection, jurisdiction and the choice of law," *Privacy Laws and Policy Reporter*, vol. 6, pp. 92-98, 1999.

[15] K. Stylianou, "An evolutionary study of cloud computing services privacy terms," *John Marshall Journal of Computer and Information Law*, vol. 27, no. 4, pp. 593, 2010.

[16] J. Soma, M. Nichols, M. M. Gates, and A. Gutierrez, "Chasing HASING the clouds without getting drench: a call for fair practices in cloud computing services," *Journal Techology, law & Policy*, vol. 16, no. 2, pp. 193-343, 2011.

[17] N. J. King and V. Raja, "Protecting the privacy and security of sensitive customer data in the cloud," *Computer Law and Security Review*, vol. 28, no. 3, pp. 308-319, 2012.

[18] W. Robison, "Free at what cost? cloud computing privacy under the stored communications act," *Georgetown Law Jornal*, vol. 98, no. 4, pp. 10, 2010.

[19] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in *Proc. IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)* 2010, pp. 693-702.

[20] H. R. M. Nezhad, B. Stephenson, and S. Singhal. Outsourcing business to cloud computing services: Opportunities and challenges. [Online]. Available: http://www.lrr.in.tum.de/~gerndt/home/Teaching/CloudComputing/20111006112649503.pdf

[21] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing—The business perspective," *Decision Support Systems*, vol. 51, no. 1, pp. 176-189, 2011.

[22] S. Sandeen, "Lost in the cloud?: the implications of cloud computing," *Trade Secret Protection*, vol .4, no.2, pp. 100-121, 2012.

[23] R. Glott, E. Husmann, A. R. Sadeghi, and M. Schunter, "Trustworthy clouds underpinning the future internet," *The Future Internet*, vol. 6656, pp. 209-221, 2011.

[24] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication 800-145, 2011.

[25] W. K. Hon, C. Millard, and I. Walden, "Who is responsible for 'personal data'in cloud computing?—The cloud of unknowing, Part 2," *International Data Privacy Law*, vol. 2, no. 1, pp. 3-18, 2012.

[26] J. Miller and D. Hoffman, "Sponsoring trust in tomorrow's technology: towards a global digital infrastructure policy," *International Data Privacy Law*, vol. 1, no. 2, pp. 83-91, 2011.

[27] M. Porter and M. R. Kramer, "Creating shared value," *Harvard business review*, vol. 89, no.1/2, pp. 62-77, 2011.

[28] L. Kogan, "Coherent international trade policies hasten, not retard, cloud computing," *Global Trade and Customs Journal*, vol. 7, no. 9, pp. 19, 2012.

[29] F. Gilbert, "European data protection 2.0: new compliance requirements in sight-what the proposed EU data protection regulation means for us companies," *Santa Clara Computer and High Technology Law Journal*, vol. 28, no. 4, pp. 815-825,2012.

[30] R. Wong, "The Data Protection Directive 95/46/EC: idealisms and realisms," *International Review of Law, Computers and Technology*, vol. 26, no. 2-3, pp. 229-244, 2012.

[31] J. Knudsen and J. Moon. (2012).Corporate social responsibility as mutual governance: International interactions of government, civil society and business. [Online]. Available: http://ssrn.com/abstract=2139861 or http://dx.doi.org/10.2139/ssrn.2139861.

[32] N. Bernaz, "Enhancing corporate accountability for human rights violations: is extraterritoriality the magic potion?" *Journal of Business Ethics*, pp. 1-19, Nov. 2012.

[33] S. Bradshaw, C. Millard, and I. Walden, "Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services," *International Journal of Law and Information Technology*, vol. 19, no. 3, pp. 187-223, 2011.

[34] A. J. Casey and S. Holmes, "Walking from cloud to cloud: the portability issue in cloud computing," *Washington Journal of Law, Technology & Arts University of Washington School of Law*, vol. 6, no. 1, pp. 1, 2010.

[35] C. Everett, "Cloud computing–a question of trust," *Computer Fraud and Security*, vol. 9, no. 6, pp. 5-7, 2009.

[36] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50-58, 2010.

[37] D. Couillard, "Defogging the cloud: applying fourth amendment principles to evolving privacy expectations in cloud computing," *Minnesota Law Review*, vol. 93, pp. 2205, 2009.

[38] P. Chynoweth, *Legal Research, Advanced Research Methods in the Built Environment*, Wiley-Blackwell, Oxford, 2008, ch.3, pp. 28-38.

[39] C. Cappa, "Model for the Integration of Legal Research into Australian Undergraduate Law Curricula," *A Legal Educ. Rev.*, vol. 14, pp. 43, 2003.

Abdallah Abuoliem is a Ph.D candidate in Department of Accounting and Corporate Governance, Faculty of Business and Economics at Macquarie University, Master of International Trade and Commerce Law, LLB in law, previously employed by Suncorp-Metway Group, Australia. He accomplished an intensive legal study and experience in the field of bilateral investment treaties, international banking and finance law, technology law.

Mr AbuOliem was awarded many achievement awards, over the past few years, recognising his excellence and commitment to improved business outcomes. His research interest includes internet content distribution, freedom of expression, foreign investment and personal data protection. Abdallah is an active member of NSW Young Lawyer Society..