Court File No.: _____

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL OF BRITISH COLUMBIA**)**

B E T W E E N:

DEBORAH LOUISE DOUEZ

APPLICANT
(Respondent)

- and -

FACEBOOK, INC.

RESPONDENT
(Appellant)

AFFIDAVIT OF TAMIR ISRAEL
(Sworn September 11, 2015)
(in support of application for leave to appeal)

I, **TAMIR ISRAEL**, of the City of Ottawa, in the Province of Ontario, DO SOLEMNLY AFFIRM THAT:

INTRODUCTION

1. I am Staff Lawyer at the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) hosted at the Centre for Law, Technology and Society (CLTS) at the University of Ottawa's Faculty of Law. I am a member in good standing of the Law Society of Upper Canada. This Affidavit is sworn in support of the Applicant's Application for Leave to Appeal, and for no improper purpose.

2. Except as otherwise indicated, I have personal knowledge of the matters to which I depose in this Affidavit. Where I lack such personal knowledge, I have indicated the source of my information and I verily believe such information to be true. Where specific CIPPIC activities are referred to below in which I have had no personal participation, I have reviewed the relevant files and base my account thereof on this knowledge.

3. I began working with CIPPIC in 2008 as a Student-at-law and Law Foundation of Ontario Public Interest Articling Fellow. I kept that position until 2009, at which time I was called to the bar of Ontario and became Staff Lawyer at CIPPIC, a position which I have since held. In addition to my work with CIPPIC, I also lecture on the regulation of e-commerce at the University of Ottawa's Faculty of Graduate and Post-Doctoral Studies. I am a member of the advisory board of Privacy International, the Mozilla Foundation's Public Policy Development Sub-Module and the Canadian Journalists for Free Expression's (CJFE) Digital Issues Committee. My experience is outlined in greater detail in my curriculum vitae, attached as Exhibit 1 to this Affidavit.

4. CIPPIC is a legal clinic founded by the University of Ottawa, Faculty of Law. It was established in September 2003 with funding from the Ontario Research Network on Electronic Commerce and an Amazon.com *Cy Pres* fund. In 2007, CIPPIC received additional funding from the Samuelson-Glushko Foundation, enabling CIPPIC to join the international network of Samuelson-Glushko technology law clinics as Canada's sole representative. CIPPIC performs its services free of charge to its clients.

5. CIPPIC operates under a Director, presently David Fewer, and a Staff Lawyer, presently myself. Both the Director and Staff Lawyer are called to the bar of Ontario and work for CIPPIC full time. CIPPIC reports to an internal Advisory Committee made up of eight faculty members who are leaders in the field of law and technology, and benefits from the expertise of an external Advisory Board composed of five highly respected and accomplished lawyers and academics in the technology law field from across North America.

6. CIPPIC's core mandate is to ensure that the public interest is accounted for in policy and legal decision-making on issues raised at the intersection of law and technology. It has the additional mandate of providing legal assistance to under-represented organizations and individuals on law and technology issues, as well as a teaching mandate focused on providing law students high quality experience and practical training in a law and technology setting. In pursuit of these mandates, CIPPIC is deeply involved in research and advocacy on the nature and social impact of online activity and the potential impact laws

can have on such activity. Its expertise has evolved through its varied advocacy on this front – advocacy which includes interventions in various levels of court, expert testimony before parliamentary committees, involvement in Internet governance related matters before various quasi-judicial tribunals and international fora, and the publication of academic and research reports on Internet law related issues.

7. The multi-lateral nature of CIPPIC's activities has furnished it with expansive institutional expertise on technology law issues, allowing it to leverage a cross-disciplinary understanding of such issues and their impact. The nature of digital innovation and technological development, which implicates privacy to historically unprecedented levels, has made privacy and data protection a substantial area of focus for CIPPIC's work. As most Internet services are global in nature, this has often involved grappling with the cross-jurisdictional aspects of privacy protection and of e-commerce more generally.

8. An indicative selection of CIPPIC's legal and policy work in relation to cross-jurisdictional e-commerce and privacy includes the following (not in chronological order):

- **House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) Study on Privacy and Social Media, June 19, 2012:** CIPPIC testified on the evolving privacy implications of social media and provided input on the need to enforce Canadian standards, including in light of the cross border nature of social networking sites and other e-commerce services;

- **OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data 30 Year Review:** by its membership in the Civil Society Information Society Advisory Council to the OECD, CIPPIC participated actively in the recent revision of the OECD Privacy Guidelines, a seminal internationally recognized standard for domestic and transborder data protection and one of the source documents on which Canada's privacy regulatory regime is premised. CIPPIC's participation included active input into provisions designed to navigate cross-border coordination of data protection regimes;

- ***Lawson v Accusearch*, 2007 FC 125:** CIPPIC sought judicial review of the Office of the Privacy Commissioner of Canada's decision to refuse on jurisdictional grounds to exercise its investigatory mandate against a company based in the United States, but allegedly violating the privacy of Canadians under Canadian law. CIPPIC successfully argued that in an online world, physical territorial location cannot immunize an organization from the privacy protections guaranteed to Canadians by the *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 [PIPEDA], Canada's federal private sector privacy legislation;

- ***Canadian Internet Policy & Public Interest Clinic v. Facebook*, PIPEDA Case Summary #2009-008:** a complaint under the *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 [PIPEDA] against Facebook, Inc., which resulted in a comprehensive overhaul of the privacy practices of that social networking site in order to comply with Canadian privacy standards;

- ***Dell Computer Corp v Union des consommateurs*, [2007] 2 SCR 801, 2007 SCC 34:** CIPPIC intervened in this appeal on the enforceability of hyperlinked mandatory arbitration clauses in e-commerce platforms;

- **ICANN, Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service, June 2014:** Advised on generating civil society input into the Expert Working Group (EWG)'s development of a mechanism for managing privacy and identification for domain registration activities overseen by ICANN. Submissions related to the nature of privacy in identification and into challenges in establishing a global, cross-jurisdictional standard;

- **"Trade in Services Agreement, E-Commerce Chapter, An Analysis", WikiLeaks.org, June 3, 2015:** An analysis of proposed text being negotiated as part of a trade partnership, including of the implications of provisions that would prevent data territorial localization as a means of shielding data from foreign state laws;

- **"Jurisdictional Issues Arising from Attempts to Incorporate Information Stored in the Cloud into Domestic Legal Processes"*, Internet Governance Forum 2012: Baku*, November 7, 2012:** hosted jointly with the Electronic Frontiers Foundation in Baku, Azerbaijan, and explored, amongst other matters, the impact of cross-border cloud services on the ability to protect data against state intrusion;

- **PIPEDA Case Summary #2008-394, *Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers*:** a complaint under the *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 [PIPEDA] against Canada.com, a service operated by Canwest Global Communications Corporation, regarding its decision to outsource the processing and storage of its email services to a company based in the United States and subject to the lawful access rules of that state;

- **"Emerging Business, Consumer & Regulatory Issues in Online Advertising", Ottawa, October 1, 2013:** a full day conference co-hosted with the Competition Bureau of Canada which explored, among other matters, the need for effective trans-jurisdictional enforcement and cooperation to meet the challenges posed by cross-border digital services;

- **Telecom Notice of Consultation CRTC 2012-557, *proceeding to establish a mandatory code for mobile wireless services*, October 11, 2012, CRTC Reference No.: 8665-C12-201212448:** a regulatory proceeding which examined, among other things, challenges arising from managing jurisdiction conflicts in

consumer protections within Canada and at the federal level;

In addition, CIPPIC has advised a number of individual and institutional clients on privacy issues arising from the operation and or storage of data in transborder contexts.

I. Contracting out of Privacy Protection

9. Privacy is a social value of growing importance as well as a human right protected in several international instruments, including most notably in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), the two most widely adopted human rights instruments. Article 17 of the ICCPR recognizes the right to legal protection against any unlawful or arbitrary interference with the right to privacy.

10. In Canada, privacy is a constitutional value intricately linked to the well being, dignity and autonomy of individuals and protected by sections 7 and 8 of the *Charter*. Canadian courts have recognized the importance of privacy as an animating legal value, and that the common law should develop in a manner that is consistent with and protective of the right to privacy. Canadian legislation that is designed to protect privacy is treated as quasi-constitutional, giving it pre-eminence over ordinary legislative initiatives in recognition of the important interests being protected.

11. The ability of individuals to protect their right to privacy has never been under greater stress than in the digital age. A recent survey commissioned by the Office of the Privacy Commissioner of Canada found that while most respondents indicated high levels of concern for privacy, 73% felt they have less capacity to protect their personal information than they did ten years ago and 60% indicated that the privacy threats they face in the world today have left them with minimal factual, as opposed to normative, expectation of privacy.[1]

12. These perceptions are in line with the exigencies of a digital world where private information must pass through a growing number of digital intermediaries who have the technical

[1] Phoenix Strategic Perspectives Inc., "2014 Survey of Canadians on Privacy: Prepared for the Office of the Privacy Commissioner of Canada", Office of the Privacy Commissioner of Canada, December 2014, Exhibit 2 (select excerpts), pp. 11 and 13.

capacity and incentive to collect and use that information through increasingly sophisticated techniques. As the United States Federal Trade Commission (FTC) recently concluded following a detailed examination of privacy in the modern age:

> Changes in technology and the emergence of new business models also have new implications for consumer privacy. For example, technological advancements and increased computing power have allowed companies to collect, store, manipulate, and share ever-increasing amounts of consumer data at very little cost. This has led to an explosion of new business models that depend upon capturing consumer data at a specific and individual level and over time, including online behavioral advertising, social media services, and location-based mobile services. … These developments can provide enormous benefits to consumers … At the same time, the enhanced ability to collect and store consumer data has increased the risks that data will be shared more broadly than understood or intended by consumers or used for purposes not contemplated or disclosed at the time of collection.[2]

Today, personal data is exposed to a greater number of parties and is increasingly valuable to such entities for a range of secondary business reasons wholly unrelated to the primary interaction undertaken by the end user.[3] The primary driver for this shift is the growing inherent economic value of personal information, which has led to its commoditization. In addition, a host of other objectives related to increased efficiency, product testing, and gauging of public attitudes incentivize each entity in the digital communications chain to maximize their collection, use and disclosure of personal information, with serious potential implications for individual privacy.

13. Private information collected by these means is also increasingly being used to make decisions that affect individual lives in significant ways, and can be determinant of insurance premiums, employment prospects, and the news or other content one is exposed to online. The privacy stakes have never been higher, elevating the importance of privacy rights and their protection. The evolving importance of privacy rights is reflected in the growing number of countries that have adopted data protection laws – 99

[2] United States Government, Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers", Preliminary FTC Staff Report, December 2010, Exhibit 3 (select excerpts), p. 21.
[3] House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), Privacy and Social Media in the Age of Big Data, 1st Session, 41st Parliament, April 2013, Exhibit 4 (select excerpts), p. 8.

in total, with 58 adopting such laws since 2000.[4] However, significant variation remains in the nature and scope of privacy protection.

14. This variation has been the source of significant concern. It applies to fundamental privacy concepts, including what constitutes a privacy 'harm', what constitutes anonymous (and therefore, unprotected) information and what constitutes consent. Recognizing this, the 35th International Conference of Data Protection and Privacy Commissioners, an annual meeting of privacy regulators from across the globe, adopted a resolution in 2013 calling on governments to develop and adopt globally applicable standards for privacy protection under Article 17 of the ICCPR, observing that:

> ... there is a pressing need for a binding international agreement on data protection that safeguards human rights by protecting privacy, personal data and the integrity of networks and enhances the transparency of data processing while striking the right balance in respect of security [sic] economic interests and freedom of expression.[5]

The lack of standardization inherent in the status quo heightens the impact that can occur when national standards do not prevail. The majority of Internet services used by Canadians are based outside of Canada, while forum selection clauses are commonly employed features of the service agreements employed by these entities. Yet the lack of standardization provides minimal guarantee of adequate protection in the jurisdiction of choice. Indeed, many Internet sites leverage the global connectivity of the medium to choose jurisdictions with minimal privacy protection with the objective of avoiding meaningful safeguards.

15. Allowing services that have substantial presence in Canada to effectively 'contract out' of Canadian law would greatly hinder the protection of Canadian privacy, frustrating an important area of public policy. The impact of permitting social networking sites with large Canadian penetration to avoid Canadian privacy standards were recently explored by the House of Commons Standing Committee on Access to Information, Privacy &

[4] G. Greenleaf, "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", (2014) 23(1) *J Law, Information & Science* 4, Exhibit 5, pp. 11-12.
[5] 35th International Conference of Data Protection Commissioners, Resolution on Anchoring Data Protection and the Protection of Privacy in International Law, Warsaw, Poland, September 2013 (United States Government, Federal Trade Commission abstaining), Exhibit 6.

Ethics (ETHI) in a study on privacy & social media. The Committee concluded that, while there may be legitimate reasons for such sites to prefer foreign laws, Canadian users of such sites should be able to benefit from Canadian standards:

> As a result of this testimony, the Committee is concerned that major social media companies, while doing business in Canada, prefer to be governed by laws other than those of this country. While the reasons for this may be economic, linguistic or business in nature, it is important that Canadians who use these services be protected by their own laws and values.[6]

A particular concern raised by the ETHI committee in its study relates to differing definitions of what constitutes 'personal information'. Some jurisdictions, such as the United States, have historically adopted a narrow definition of this term, requiring the inclusion of a name or other recognized identifier in an interaction before a privacy interest can be invoked. However, most other jurisdictions (including Canada) have recognized that in the digital world a significant range of potentially invasive activity occurs without the use of traditional identifiers. Additional important variations between Canadian and United States privacy standards relate to what constitutes a legally salient privacy 'harm' and to the use of more rigorous definitions of 'consent' under Canadian privacy laws.[7]

16. The obligation to obtain meaningful individual consent is a centerpiece of Canadian privacy protection. Under Canadian privacy law, consent is required out of recognition that contractual assent leads to a 'take it or leave it' approach that fails to safeguard privacy interests.[8] The United States Federal Trade Commission has recently recognized the shortcomings of this approach, commonly referred to as the 'notice and choice model':

> Participants also pointed to shortcomings in existing frameworks that have attempted to address privacy concerns. The "notice-and-choice model," which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand. … Participants noted that both of these privacy frameworks have struggled to

[6] House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), Privacy and Social Media in the Age of Big Data, 1st Session, 41st Parliament, April 2013, Exhibit 4 (select excerpts), p. 7.
[7] United States Government, Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers", FTC Report, March 2012, Exhibit 7 (select excerpts), p. 2.
[8] House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), Privacy and Social Media in the Age of Big Data, 1st Session, 41st Parliament, April 2013, Exhibit 4, p. 16.

> keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers. … Building on the record developed at the roundtables and on its own enforcement and policymaking expertise, FTC staff proposed for public comment a framework for approaching privacy. … The proposed framework also called on companies to simplify consumer choice by presenting important choices – in a streamlined way – to consumers at the time they are making decisions about their data.[9]

While contracts of adhesion are rarely read in any context, this is all the more so in the context of services that depend on personal information for monetization. The long term privacy harms that result from such services can be significant, but the immediate cost is negligible, meaning that customers will not approach such services with the care that they might approach a mortgage or car rental agreement. Moreover, as individuals encounter many of these services on any given day, the time and effort it would take the most diligent customer to audit the terms of service and privacy policies of each is insurmountable.[10]

17. Forum selection clauses can have serious implications for Canadian privacy, as they effectively contract individuals out of Canadian legal standards. Foreign courts will predominantly apply domestic law in the absence of an enforceable choice of law clause or overriding public policy concern.[11] However, while Canadian law recognizes the constitutional importance of privacy in the commercial sector, United States law does not accord it the same level of public policy importance, resulting in jurisprudence that is unlikely to forgo local laws in order to safeguard privacy.[12] Such clauses are typically imposed onto customers of e-commerce platforms in contracts of adhesion, without any right of refusal or enhanced notification. They operate to confound the privacy expectations of customers, who expect to enjoy the protections offered by Canadian law

[9] United States Government, Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers", FTC Report, March 2012, Exhibit 7, p. 2.
[10] A.M. McDonald and L.F. Cranor, "The Cost of Reading Privacy Policies", (2008) *I/S: A Journal for Law and Policy for the Information Society*, 2008 Privacy Year in Review Issue, Exhibit 8.
[11] J. Delisle & E Trujillo, "Consumer Protection in Transnational Contexts", (2010) 58 *American J of Comparative L* 135, pp. 146-47, Exhibit 9 (select excerpts); T. Scassa and R.J. Currie, "New First Principles? Assessing the Internet's Challenges to Jurisdiction", (2011) 42 *Georgetown J of International Law* 1017, Exhibit 10, pp. 1062-63; *Equustek Solutions Inc v Google Inc*, 2015 BCCA 265, paras 91-92.
[12] A. Levin & M.J. Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground", (2005) 2(2) *University of Ottawa L & Technology J* 357, Exhibit 11, generally and pp. 367-68, specifically; T. Scassa and R.J. Currie, "New First Principles? Assessing the Internet's Challenges to Jurisdiction", (2011) 42 *Georgetown J of International Law* 1017, Exhibit 10, pp. 1058-60; *Yahoo! Inc v La Ligue contre le racism et l'antisémitisme* (2006), 433 F.3d 1199 (United States, 9th Cir., *en banc*).

in the activities and interactions with other Canadians that are facilitated by these digital platforms.

II. Contracting out of Rights-Protecting Mechanisms

18. Forum selection clauses pose a particular challenge for the protection of privacy in a cross-border world. However, forum selection clauses can also frustrate other important public policy objectives. In particular, a number of Canadian provinces have taken steps to secure appropriate fora and procedural mechanisms for various consumer protection rights. This includes: granting consumers the inalienable right to have certain statutory claims heard before a superior court of record,[13] regulating the enforceability of mandatory arbitration clauses,[14] and rendering the use of class action waivers unenforceable in consumer contracts.[15] These protections set important standards for consumers and help instill trust in e-commerce in general. However, United States law has been criticized for not permitting bans on mandatory arbitration clauses in contracts of adhesion.[16] This is so even where the use of such clauses is used as a tool to effectively prevent class claims by mandating individual arbitration of claims.[17]

III. Regulation of cross-border e-commerce and forum selection clauses in general

19. E-commerce is a rapidly evolving field that is beginning to effect increasingly significant portions of Canadian life. The day to day operation of automobiles, home televisions, refrigerators, light switches and home alarm systems are all projected to become regular staples of e-commerce platforms in the next five to ten years. In this landscape, it is difficult to predict what customer harms may arise in the future and how these will be addressed by Canadian jurisdictions and abroad. However, it is inevitable that e-commerce will continue to include the capacity to impose contracts of adhesion that are

[13] *Business Practices and Consumer Protection Act*, SBC 2004, c 2, section 172. *Privacy Act*, RSBC 1996, c 373, section 4.
[14] *Consumer Protection Act, 2002*, SO 2002, c 30, Sch A, sub-section 7(2); *Consumer Protection Act*, RSQ, c P-40.1, section 11.1; *Griffin v Dell Canada Inc*, 2010 ONCA 29.
[15] *Consumer Protection Act, 2002*, SO 2002, c 30, Sch A, sub-section 8(1); *Consumer Protection Act*, RSQ, c P-40.1, section 11.1
[16] Public Citizen and National Association of Consumer Advocates, "Justice Denied: One Year Later: The Harms to consumers from the Supreme Court's *Concepcion* Decision are Plainly Evident", April 2012, Exhibit 12.
[17] Public Citizen and National Association of Consumer Advocates, "Justice Denied: One Year Later: The Harms to consumers from the Supreme Court's *Concepcion* Decision are Plainly Evident", April 2012, Exhibit 12.

rarely read by consumers and it will continue to include cross-border provision of services. These are persistent features of the e-commerce landscape, and they guarantee that forum selection clauses – if widely enforceable – will continue to play a central role in determining the capacity of Canadian policy makers to establish public policy standards for Canadians in this area of growing importance.

Conclusion

20. In conclusion, the enforcement of forum selection clauses in the e-commerce context can have serious and detrimental implications for Canadian public policy, implications that are particularly significant in the privacy context. Should leave to appeal be granted by the Supreme Court of Canada, CIPPIC intends to seek leave to intervene in order to present arguments concerning this matter.

SWORN before me at the City of Ottawa)
in the Province of Ontario)
this 11th day of September, 2015)

TAMIR ISRAEL

_____

Commissioner for Taking Oaths