"ESSENTIAL EQUIVALENCE" AND EUROPEAN ADEQUACY AFTER *SCHREMS*:

THE CANADIAN EXAMPLE

GABE MALDOFF AND OMER TENE*

ABSTRACT

In *Schrems v. Data Protection Commissioner*, the Court of Justice of the European Union found that national security surveillance by foreign countries undermines the privacy rights of Europeans. In so finding, the Court struck down the most important data transfer mechanism between the European Union and the United States. Much more than just derailing the EU-US Safe Harbor arrangement, this could spell the demise for every legal mechanism used to transfer data out of Europe, with significant implications on global trade. A challenge to standard contractual clauses has already been brought before the Court of Justice. Existing adequacy determinations for transfers to other countries could also be at risk, as it is doubtful that the European Commission explored government access when approving them. In the early 2000s, Canada gained adequate status on the basis of the Personal Information Protection and Electronic Documents Act (PIPEDA), an omnibus privacy law designed to keep pace with Europe and assure access to its market. But PIPEDA focused only on the data handling practices of Canada's private sector, without limitations on national security access. Now it too seems vulnerable to the same attack. This article looks at Canada as a test case for the resilience of the other existing adequacy regimes. By exploring the national security apparatus in Canada, this article examines the new test for adequacy that flows from the *Schrems* ruling.

* Gabe Maldoff is a Westin Fellow at the International Association of Privacy Professionals; Omer Tene is Associate Professor, College of Management School of Law, Rishon Lezion, Israel.

ABSTRACT 211
Background 213
I. The Data Protection Directive and International Data Transfers 213
II. PIPEDA and Canada's Adequacy Determination 217
III. EU-US Safe Harbor 221
IV. How We Got Here: The Fall of Safe Harbor 224
A. Edward Snowden and the Max Schrems Story 225
1. Revelations of Secret Surveillance 225
2. Max Schrems Takes on Facebook 227
B. Schrems v. Data Protection Commissioner 230
1. The Role of Data Protection Authorities 230
2. Limits to Surveillance 231
C. Measuring Adequacy: Essentially Equivalent to What? 233
1. Interpretation of the EU Charter is Informed by the Jurisprudence of the European Court of Human Rights 235
2. Privacy Shield as the New Standard for Adequacy? 236
3. Crafting a Standard 238
V. Canadian National Security Safeguards 240
A. The Royal Canadian Mounted Police ("RCMP") 240
B. The Canadian Security Intelligence Services ("CSIS") 243
C. The Communications Security Establishment ("CSE") 246
D. Data Retention and Information Sharing 247
1. Analysis of Canadian Safeguards 249
E. Clear, Precise, and Accessible Rules 249
1. The Application of the Canadian Charter of Rights and Freedoms to Foreign Searches is Unsettled 250
2. Government Interception of Non-Private Communications Is Not Subject to Clear, Precise and Accessible Rules 254
3. Canada's Framework May Be Circumvented by Cooperation with the "Five Eyes" and Boomerang Routing 256
F. Strictly Necessary and Proportionate 259
1. Interception of Foreign-to-Foreign Communications Abroad 260
2. Interception of European-Canadian Communications 262
3. Interception of Communications Metadata 267
4. Access to Stored Communications and Business Records 271

5. Data Retention and Information Sharing 274
G. Independent Oversight 275
H. Effective Redress 278
VI. Conclusion 281

BACKGROUND

I. THE DATA PROTECTION DIRECTIVE AND INTERNATIONAL DATA TRANSFERS

On July 25, 1995, the European Union ("EU") formally enacted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, known as the Data Protection Directive.[1] Effective in 1998, the Data Protection Directive required each EU Member State to impose restrictions on the processing of personal data to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy."[2]

The Data Protection Directive aimed to reconcile the conflicting standards of data protection that had emerged in a number of EU Member States. Before the Data Protection Directive, EU data protection law was composed of a series of Member State statutes that were passed in the 1970s, beginning with a Länder-level law in Germany.[3] Some of these statutes explicitly prohibited the transfer of personal data to other countries—including other European Countries—that did not provide "equivalent protection."[4] Other statutes banned international data

---

1 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, art. 25, 1995 O.J. (L 281) [hereinafter Data Protection Directive].

2 *Id.* at art. 1.

3 Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1969 (2013) [hereinafter Schwartz, *Privacy Collision*].

4 Lei da Protecção de Dados Pessoais face à Informática [Law for the Protection of Personal Data with Regard to Automatic Processing], Law 10/91, art. 33 (1991) ("uma protecção equivalente") (Port.); Ley Organica 5/1992 de 29 de octubre, de regulacion del tratamiento automatizado de los datos de caracter personal [Law on the Regulation of the Automatic Processing of Personal Data], 10/92, art. 32 (1992) ("un nivel de protección equiparable al presta") (Spain).

transfers altogether in the absence of further legislation permitting such transfers.[5]

By the late 1970s, the need for a harmonized approach had become evident. The Organisation for Economic Co-operation and Development (OECD) recognized that "differing national legal regulations, superimposed on interconnecting communications technology, would produce serious inefficiencies and economic costs."[6] To address the potential for economic disruption, the OECD released a set of Guidelines on the protection of personal data that encouraged member countries to "refrain from restricting transborder flows of personal data . . . except where the latter does not yet substantially observe [the OECD] Guidelines."[7] One year later, the Council of Europe's Data Protection Convention sought to promote "free flows of data"[8] among countries that were signatories to the treaty,[9] while still allowing signatory countries to block transfers to non-signatory countries that did not provide "equivalent protection."[10]

The 1995 Data Protection Directive harmonized the disparate legislative frameworks in the EU by requiring each EU Member State to implement specific principles for data processing.[11] The Data Protection

---

5 *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 Iowa L. Rev. 471, 478 (1995) [hereinafter Schwartz, *Data Protection Law*] (explaining that the French and Belgian statutes forbade transfers to any third country without expressing an explicit standard by which to evaluate another country's legislation).

6 Michael Kirby, *Remarks on the 30th Anniversary of the OECD Privacy Guidelines*, Thirty Years After: The OECD Privacy Guidelines 8 (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf. When the OECD revised its guidelines in 2013, harmonizing international data transfers remained a significant focus of the initiative. *See* Org. for Econ. Co-operation & Dev. [OECD], *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, preface (2013), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (warning that "there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers," especially given that "these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology").

7 Org. for Econ. Co-operation & Dev. [OECD], *Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, art. 17, C(80)58/FINAL, (Oct. 1, 1980) [hereinafter OECD Guidelines], http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf.

8 Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, pmbl., Jan. 28, 1981, E.T.S. No. 108, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

9 *Id.* at art. 12.

10 *Id.* at art. 12(3)(a).

11 Schwartz, *Data Protection Law*, *supra* note 5, at 480.

Directive applied to private and public entities alike, imposing strict requirements on all organizations that process personal data, with an exemption when "a restriction constitutes a necessary measure to safeguard," *inter alia*, national security, defense, and public security.[12] It created "supervisory authorities" in each State (often referred to as "Data Protection Authorities" or "DPAs"), empowered to "act with complete independence" in overseeing personal data processing operations, and it mandated the free flow of data within the EU.[13]

These robust protections would have been meaningless, however, if they could be easily circumvented by transferring data outside the EU. Given that data moves readily around the globe with negligible cost and at the speed of light, the EU needed to put in place virtual border controls to maintain the integrity of its framework. To resolve this, the Data Protection Directive introduced the concept of "adequacy."[14]

Article 25 of the Data Protection Directive forbade the transfer of personal data to a third country outside the EU, unless that country offers "an adequate level of protection."[15] Each Member State's supervisory authority was empowered to determine the adequacy of a third country's protections "in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations."[16] The Data Protection Directive also created a mechanism by which the European Commission could find that a third country offered adequate protections "by reason of its domestic law or of the international commitments it has entered into."[17] Such a finding would permit the transfer of data from any EU Member State to that third country.[18]

The Data Protection Directive also established several other mechanisms, including standard contractual clauses and unambiguous consent, to facilitate cross-border data transfers. These mechanisms

---

[12] Data Protection Directive, *supra* note 1, art. 13(1).

[13] *Id.* at art. 28(1).

[14] Schwartz, *Data Protection Law*, *supra* note 5, at 473.

[15] Data Protection Directive, *supra* note 1, art. 25(1).

[16] *Id.* at art. 25(2) (stating that assessment of a third country's adequacy should include "the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.")

[17] *Id.* at art. 25(6).

[18] *Id.*

allowed organizations to transfer personal data to third countries, even if those countries had not been found adequate.[19] However, unlike adequacy findings, these mechanisms were cumbersome for organizations that transfer personal data. For example, to use a standard contractual clause, an organization was required to implement detailed contractual language, approved by Member State regulators, in its relationship with any other entity handling the data. These contractual relationships extended European-style data protection requirements to all the entities involved in data processing. For a large conglomerate, this meant hundreds or even thousands of contracts had to be put in place and revised regularly. An additional mechanism, called Binding Corporate Rules (BCRs), grew out of the need for a more streamlined, efficient process.[20] BCRs allowed an organization to submit its practices for detailed auditing by regulators, in a process that could take several years but saved the organization the need to implement, monitor and revise innumerable contractual arrangements.

Because of the ease of transferring data to an "adequate" jurisdiction, adequacy remained the Holy Grail. Alas, only a handful of countries were successful in obtaining the seal of adequacy. Among the world's developed economies, only Canada, Israel, New Zealand, and Switzerland secured adequate status, as well as the United States under a more limited framework, outlined below. Important partners such as Japan and Australia were excluded, as were massive trading blocs such as China and India.

As the growth of information services in the 2000s raised the prospect of greater economic integration, the EU placed increased emphasis on legal privacy protections, especially for online activities.[21] The Charter of Fundamental Rights of the European Union ("EU Charter") became legally binding with the Lisbon Treaty's entry into

---

[19] *Id.* at art. 26.

[20] Lokke Moerel, Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection 19-27 (2011).

[21] *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protective of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), (L 201) (EC). *See also* Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services); Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, (L 364) (applying security and confidentiality requirements to digital technologies as well as placing restrictions on the use of browser cookies).

force in 2009.[22] The EU Charter enshrined, in Article 7, the right to respect for a person's "private and family life, home and communications."[23] Article 8's right to "protection of personal data" provided individuals with the right to have their personal data "processed fairly and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[24]

Relying on the EU Charter, the Court of Justice of the European Union (CJEU) became an important arbiter of privacy rights, handing down major privacy decisions.[25] In one 2014 decision, *Digital Rights Ireland and Others*, a case that would become central to defining "adequacy," the Court invalidated the EU Data Retention Directive, which had required telecommunications service providers to retain subscriber and location data so as to be accessible to public authorities investigating "serious crimes."[26] Relying on Articles 7 and 8 of the EU Charter, the Court held that the retention of the data, and access to it by national authorities, "constitutes a particularly serious interference with those [EU Charter] rights."[27] Thus, after *Digital Rights Ireland*, it became clear that the EU Charter compelled a strict reading of the national security, defense, and public security exemptions to the Data Protection Directive.[28]

II. PIPEDA AND CANADA'S ADEQUACY DETERMINATION

Canada's protections for personal data privacy began in the 1970s, when Canadian courts first recognized a "human right" to control

---

[22] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364/01) [hereinafter EU Charter].

[23] *Id.* at art. 7.

[24] *Id.* at art. 8(2).

[25] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R. 317 (establishing a "right to be forgotten" that required search engines to remove embarrassing links to a person's name upon that person's request).

[26] Case C-293/12, Dig. Rights Ir., Ltd. v. Minister for Commc'n, 2014 E.C.R. 238, [hereinafter Digital Rights Ireland], http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d55a61733fca5a4dcb93b7a9ae50b99d00.e34KaxiLc3eQc40LaxqMbN4Pa3aSe0?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=340236.

[27] *Id.* ¶ 39.

[28] *Id.* ¶ 48.

one's personal information.[29] Shortly thereafter, several provinces enacted statutes that permitted privacy tort actions.[30] In 1982, Canada adopted the Charter of Rights and Freedoms into its constitution, which enshrined, in Section 8, a "right to be secure against unreasonable search or seizure."[31] Citing the United States Supreme Court case, *Katz v. United States*,[32] the Supreme Court of Canada held that Section 8 protects at minimum "a 'reasonable' expectation of privacy."[33]

Canada enacted broad protections for personal information collected by the federal government and its agencies in the Privacy Act of 1985.[34] The Privacy Act created the Office of the Privacy Commissioner of Canada ("OPC") to oversee federal government compliance.[35] The provinces followed suit, enacting privacy protections for personal information collected by provincial governments.[36] In 1994, Quebec became the first jurisdiction in Canada to extend these protections to private sector entities. The Quebec act, *An Act Respecting the Protection of Personal Information in the Private Sector*,[37] was followed by similar legislation in other provinces.[38]

In response to the Data Protection Directive and the threat it posed to data transfers between Europe and Canada, Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA)[39] in 2000.[40] Modeled after the Canadian Standards Association Model Code for the Protection of Personal Information, a self-regulatory industry code, PIPEDA extended federal regulatory control over privacy

---

[29] Juliana M. Spaeth, Mark J. Plotkin & Sandra C. Sheets, Privacy, Eh!: The Impact of Canada's Personal Information Protection and Electronic Documents Act on Transactional Business, 4 VAND. J. ENT. L. & PRAC. 28, 31 (2002)

[30] *Id.*

[31] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c 11, § 8 (U.K.).

[32] Katz v. United States, 389 U.S. 347 (1967).

[33] Hunter v. Southam, [1984] 2 S.C.R 145, 146 (Can.).

[34] Privacy Act, R.S.C., 1985, c P-21.

[35] *Id.* § 53(1).

[36] *See Overview of Privacy Legislation in Canada*, OFF. OF THE PRIVACY COMM'R OF CAN., https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (last modified May 15, 2014).

[37] An Act Respecting the Protection of Personal Information in the Private Section, R.S.Q., c P-39.1 (Can.).

[38] *See, e.g.*, Personal Information Protection Act, Alta. Reg. 366/2003 (Can.); Personal Information Protection Act, S.B.C. 63/2003 (Can.).

[39] Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.) [hereinafter PIPEDA].

[40] Jennifer McClennan & Vadim Schick, "O, Privacy" Canada's Importance in the Development of the International Data Privacy Regime, 38 GEO. J. INT'L L. 669, 670–71 (2007).

to the private sector.[41] Like the Data Protection Directive, PIPEDA's framework was based on the Fair Information Practice Principles (FIPPs).[42]

At the time of its enactment, the act applied to all private sector organizations in Canada engaged in a "commercial activity."[43] PIPEDA also carved out an exception for private sector organizations that operate exclusively within a province that enacted "substantially similar" legislation, such as Quebec, Alberta and British Columbia.[44] Additionally, Ontario, New Brunswick, and Newfoundland and Labrador enacted substantially similar legislation for the protection of health information.[45] Thus, PIPEDA now applies to private sector organizations carrying on business in Canada when the personal data they collect, use or disclose crosses provincial or national borders, when they operate in provinces that have not enacted substantially similar legislation, or when the organization is federally-regulated, such as a bank, airline or telecommunications company.[46] In three provinces, it does not apply to health information.

PIPEDA also extended OPC oversight to these private sector organizations.[47] Under PIPEDA and the Privacy Act, OPC was empowered to investigate complaints and audit compliance with the acts.[48] The Privacy Commissioner reports directly to Parliament and may publish reports about personal data handling practices and promote awareness of privacy issues.[49] Before 2015, OPC could not issue binding orders or extract sanctions or fines. To seek relief against a company for non-compliance, OPC instead could apply to a Canadian federal court. In 2015, PIPEDA was amended to provide OPC with the authority to issue sanctions in limited circumstances.[50] The amendment required companies

---

41 Christopher Berzins, Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building, 27 QUEEN'S L.J. 609, 620–21 (2002).

42 *Id.*

43 A commercial activity is "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." PIPEDA, supra note 39, § 2(1).

44 Avner Levin, Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada, 22 CAN. J.L. & SOC'Y 197, 199– 200 n.10 (2007).

45 *Provincial Legislation Deemed Substantially Similar to PIPEDA*, OFF. OF THE PRIVACY COMM'R OF CAN., https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp (last modified Mar. 22, 2013).

46 *Overview of Privacy Legislation in Canada*, *supra* note 36.

47 PIPEDA, *supra* note 39, § 11(2).

48 *Id.* § 12(1).

49 *Id.* § 13(1).

50 Digital Privacy Act, S.C. 2015, c 32 (Can.).

to notify OPC and affected individuals of a data breach, with fines for non-compliance.[51] OPC also gained the authority to enter into and enforce compliance agreements with organizations falling under OPC's jurisdiction.[52]

On December 20, 2001, after reviewing Canada's privacy protections, the European Commission issued an adequacy decision finding that Canada provided an "adequate level of protection for personal data."[53] The decision applied only to private sector organizations regulated by PIPEDA.[54] It did not apply to non-profits, public entities, or private entities regulated under substantially similar provincial legislation.[55] The adequacy decision foresaw future amendment "when the Canadian Government recognizes a provincial law as being substantially similar."[56] Despite Canada's recognition of six provincial statutes as being substantially similar to PIPEDA, however, the European Commission has yet to update its adequacy decision.

Critically, the adequacy decision did not mention government access for national security purposes. In fact, PIPEDA did not even restrict such access.[57] Rather, while the law generally forbids organizations from disclosing personal information to third parties without the consent of the data subject, "an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is . . . (c.1) made to a government institution . . . that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs."[58] Thus, government access to data for

---

[51] *Id.* at 10.1(1)-(6).

[52] *Id.* at 17.1(1).

[53] Commission Decision 2002/2/EC, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act, C(2001) 4539, [hereinafter Canadian Adequacy Decision], http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002D0002&qid=1415699250815.

[54] Frequently Asked Questions on the Commission's Adequacy Finding on the Canadian Personal Information Protection and Electronic Documents Act, EUR. COMM'N, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/index_en.htm (last modified Feb. 12, 2015).

[55] *Id.*

[56] *Id.*

[57] Michael Geist & Milana Homsi, *Outsourcing Our Privacy?: Privacy and Security in a Borderless Commercial World*, 54 U. NEW BRUNSWICK L.J. 272, 297–98 (2005).

[58] PIPEDA, *supra* note 39, § 7(3).

national security purposes fell outside the scope of both PIPEDA and the European Commission's adequacy decision.

III. EU-US SAFE HARBOR

Rather than adopting omnibus privacy legislation, like the Data Protection Directive or PIPEDA, the United States opted for a different approach, creating a quilt of sector-specific federal legislation enmeshed with state laws. In the United States, for example, there are federal statutes governing health privacy,[59] financial privacy,[60] education privacy,[61] and children's online privacy,[62] as well as state-level privacy initiatives, most notably security breach notification laws,[63] and a federal statute that governs the public sector.[64] However, no federal statute regulates data privacy for private entities that fall outside of these sectors.

The United States does not limit transfers of data to other countries.[65] Cynics may argue that this is because the United States is notorious for exercising long-arm jurisdiction. In the privacy context, for example, any website directed at US children under the age of 13, regardless of its location, could be subject to enforcement under the Children's Online Privacy Protection Act (COPPA).[66] And this phenomenon is not limited to privacy laws. The Foreign Account Tax Compliance Act, for example, requires foreign financial institutions to report asset and identity information of any US persons using their services.[67] In another example, US authorities have used the Unlawful Internet Gambling Enforcement Act to target foreign-operated online

---

59 Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

60 Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); Gramm-Leach-Bliley Act, Pub. L. No. 106-102,113 Stat. 1338 (1999).

61 Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

62 The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6506.

63 Danielle Keats Citron, Privacy Enforcement Pioneers: The Role of State Attorneys General in the Development of Privacy Law, NOTRE DAME L. REV. (forthcoming 2016), http://bit.ly/2a46oAU.

64 Privacy Act of 1974, 5 U.S.C. § 552a (1974).

65 Schwartz, *Privacy Collision*, *supra* note 3, at 1977–78.

66 *FTC Warns Children's App Maker BabyBus About Potential COPPA Violations*, FED. TRADE COMM'N (Dec. 22, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa.

67 Foreign Account Tax Compliance Act of 2009, 26 U.S.C. §§ 1471-1474 (2009).

gambling sites, including PokerStars, which was founded by a Canadian.[68]

Similarly, the United States has no designated privacy regulator, akin to a European Data Protection Authority. The Federal Trade Commission ("FTC"), state attorneys general and several other federal regulators that have limited privacy mandates, including the U.S. Department of Health and Human Services Office for Civil Rights,[69] the Consumer Financial Protection Bureau,[70] and the Securities and Exchange Commission[71] have stepped in to fill this void.

The FTC has been the regulator most active in enforcing privacy protections. Under Section 5 of the Federal Trade Commission Act, the FTC has the authority to proscribe "unfair or deceptive acts or practices in or affecting commerce."[72] Section 5 allows the FTC to enforce any material promise made by a company subject to the FTC's jurisdiction.[73] Since the late 1990s, the FTC has used this authority to pursue more than 200 cases of alleged violations of consumer privacy.[74] In addition to enforcing several sectoral statutes, the FTC has encouraged companies to provide notice of their data processing activities and has held those

---

[68] Lawrence G. Walters, *The Long Arm of the Law: Can the UIGEA Be Applied to Canadian Gaming Operations?*, AMERICAN BAR ASSOCIATION, http://apps.americanbar.org/buslaw/committees/CL430000pub/newsletter/200905/chair-longarm.pdf (last visited Nov. 13, 2016); Andrew F. Cooper, *Clearing the Murky Picture of Offshore Internet Gambling*, TORONTO STAR, (May 11, 2011), https://www.thestar.com/opinion/editorialopinion/2011/05/11/clearing_the_murky_image_of_offshore_internet_gambling.html.

[69] *See generally Health Information Privacy*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/hipaa/index.html; *About Privacy at the SEC: Privacy Compliance*, U.S. SEC. AND EXCH. COMM'N, https://www.sec.gov/about/privacy/secprivacyoffice.htm (last modified Feb. 4, 2015).

[70] *Privacy*, CONSUMER FIN. PROT. BUREAU, http://www.consumerfinance.gov/privacy/ (last visited Nov. 13, 2016).

[71] U.S. SEC. AND EXCH. COMM'N, *supra* note 69.

[72] Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2012).

[73] *See* Letter from the Fed. Trade Comm'n to John D. Dingell, Chairman, Comm. on Energy and Commerce (FTC Policy Statement on Deception) (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf .

[74] *See FTC Casebook*, INT'L ASS'N PRIVACY PROF'LS, https://iapp.org/resources/ftc-casebook/ (cataloguing FTC privacy and data security enforcement actions) (last visited May 15, 2016). *See also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (arguing that FTC enforcement actions create a common law of enforceable legal norms); CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016) (cataloguing the history of the FTC's regulation of information privacy).

companies to the terms of their notice.[75] Increasingly, the FTC has used its "unfairness" authority to proscribe data handling practices that fall short of consumer expectations. State attorneys general have secured similar, and in some cases stronger, privacy protections under state-level statutes regulating "unfair or deceptive act[s] or practice[s]."[76]

Because the United States did not enact omnibus privacy legislation and had no dedicated DPA, it likely would not have met the threshold for adequacy. As a result, US officials never applied for an adequacy determination based on the US framework.[77] But, as the EU's largest trading partner, transfers to the United States simply could not be ignored. In 1998, the European Commission and the US Department of Commerce began negotiations on an alternative framework for transatlantic data flows.[78] After two years of negotiations, the European Commission released the final text of the EU-US Safe Harbor Arrangement ("Safe Harbor") on July 25, 2000.[79] The resulting framework created an "adequate" mechanism by which participating companies could transfer EU personal data to the United States.[80]

Safe Harbor operated as a voluntary self-certification program.[81] Under Safe Harbor, companies promised to adhere to the Safe Harbor Principles, which included protections similar to those of the Data Protection Directive, particularly around notice, choice, access, security, data integrity, and onward transfers to third parties.[82] Companies that wished to participate were required to certify their compliance with the Principles to the Department of Commerce and publicize their adherence to Safe Harbor in their privacy notices.[83]

---

[75] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 284–87 (2011).

[76] Citron, *supra* note 63, at 65.

[77] Peter Swire & Robert E. Litan, *Avoiding a Showdown over EU Privacy Laws*, THE BROOKINGS INSTITUTION (Feb. 1998), http://www.brookings.edu/research/papers/1998/02/europe-swire.

[78] Chuan Sun, The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective, 2 NW. J. OF TECH. & INTELL. PROP. 99, 106–7 (2003).

[79] Commission Decision 2000/520/EC, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, C(2000) 2441 [hereinafter "Safe Harbor Decision"], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=en.

[80] *Id.*

[81] Ioanna Tourkochoriti, The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance, 36 U. PA. J. INT'L L. 459, 469–71 (2014).

[82] Sun, *supra* note 78, at 107–08.

[83] Tourkochoriti, *supra* note 81, at 470.

By requiring companies to publicize their commitment to Safe Harbor, the commitment became binding and enforceable by the FTC under its Section 5 authority against deceptive trade practices.[84] To be sure, Safe Harbor did not authorize the FTC to enforce European data protection legislation. A company that failed to live up to its public promises, however, committed a "deceptive act or practice," enforceable under Section 5 of the FTC Act. From 2000 to 2015, the FTC brought cases against Google, Facebook, MySpace, and TES Franchising for violations of the Safe Harbor Principles. The FTC also brought thirty-six cases against companies that failed to renew their self-certification or that claimed Safe Harbor certification but never filed with the Department of Commerce.[85]

Neither the Safe Harbor Principles nor the European Commission's adequacy decision placed limits on national security access. In fact, the Principles stated that an organization's adherence to the framework "may be limited (a) to the extent necessary to meet national security, public interest, or law enforcement requirements, [or] (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization."[86] Hence, Safe Harbor included a broad exemption for national security access.

By 2015, more than four thousand companies of all sizes relied on Safe Harbor to transfer data.[87]

IV. HOW WE GOT HERE: THE FALL OF SAFE HARBOR

Safe Harbor was a carefully-negotiated compromise, striking a balance between divergent concepts of privacy protection.[88] Even after its

---

[84] *Id.*

[85] ANNA MYERS, INT'L ASS'N PRIVACY PROF'LS, FTC ENFORCEMENT OF THE U.S.-EU SAFE HARBOR FRAMEWORK, 9 (2015) https://iapp.org/media/pdf/resource_center/IAPP_FTC_SH-enforcement.pdf.

[86] Safe Harbor Decision, *supra* note 79.

[87] Ivana Kottasova, *Europe Cracks Down on U.S. Tech With Data Ruling*, CNN MONEY Oct. 6, 2015, http://money.cnn.com/2015/10/06/technology/facebook-privacy-european-union/. *See* U.S.-EU Safe Harbor List, https://safeharbor.export.gov/list.aspx, for a complete list of Safe Harbor-certified companies.

approval by the European Commission, EU officials as well as the FTC and advocates in the United States continued to call for federal privacy legislation to govern the commercial use of personal data.[89] But until its demise in 2015, Safe Harbor remained the most important mechanism for transferring personal data to the United States.[90]

A. EDWARD SNOWDEN AND THE MAX SCHREMS STORY

1. Revelations of Secret Surveillance

On June 5, 2013, The Guardian reported that "[t]he National Security Agency ["NSA"] is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order . . . ."[91] Over the days that followed, a series of reports in The Guardian and The Washington Post detailed aspects of the US surveillance architecture.[92] The reports revealed NSA surveillance programs directed at United States and foreign communications alike.[93] They also revealed cooperation between the NSA and several foreign intelligence agencies.[94] Within a few days of the first report, Edward Snowden, a 29-year-old NSA contractor, came forward as the source for the leaked information.[95]

---

[88] *See* Tourkochoriti, *supra* note 81, at 467 ("The differences [between the U.S. and EU approaches to privacy] concern first, the fundamental presumptions concerning the processing of personal data. The presumption in the U.S. is that the processing of personal data is permitted unless it causes harm or is limited by law. The opposite presumption is dominant in the EU where processing is prohibited unless there is a legal basis that allows it.").

[89] David A. Castor, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 IND. INT'L & COMP. L. REV. 265, 275 (2002); FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 36 (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[90] Joshua P. Meltzer, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows*, THE BROOKINGS INSTITUTION (Nov. 2015), http://www.brookings.edu/research/testimony/2015/11/03-eu-safe-harbor-decision-transatlantic-data-flows-meltzer.

[91] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[92] See G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861, 893–899 (2013) for a timeline of national security leaks beginning in 2001.

[93] *Id.*

[94] *Id.*

[95] Glenn Greenwald, Ewan MacAskill, & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 9, 2013, 9:00 AM),

Snowden's leaked documents alleged the existence of two NSA programs directed at foreign communications. The first, reported on June 6, 2013, was a top-secret NSA program called "PRISM" that, according to a leaked document, provided the NSA "direct access from the servers of these US service providers: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple."[96] The program allegedly permitted the NSA to access "records such as emails, chat conversations, voice calls, documents and more."[97] The extent of the PRISM program and the NSA's ability to directly access the contents of the servers of these companies remains a subject of debate.[98] Subsequent reports have clarified that, under the PRISM program, the NSA, by way of the FBI, sent specific selectors (such as an email or Internet Protocol (IP) address) to US-based electronic communications service providers.[99] The service provider would then be required to turn over any communications involving the selector to the NSA.[100] Notably, all of the allegedly participating companies were certified to transfer EU data to the United States under Safe Harbor.[101]

On June 8, 2013, a leak described another program, which used a technique known as upstream collection. This program allegedly enabled the NSA to collect communications on "fiber cables and infrastructure as data flows past"[102] with devices connected to high capacity cables, switches and routers that form the backbone of the internet's infrastructure. Using upstream collection, the NSA allegedly copied,

---

http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

96 Dominic Rush & James Ball, *PRISM Scandal: Tech Giants Flatly Deny Allowing NSA Direct Access to Servers*, THE GUARDIAN (June 6, 2013, 19:48), http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining.

97 *Id.*

98 Peter Swire, US Surveillance Law, Safe Harbor, and Reforms Since 2013 14–15 (2015), http://bit.ly/29oxJQk.

99 Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 33 (2014), https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB Report].

100 *Id.*

101 Tourkochoriti, *supra* note 81, at 475; The Privacy and Data Security Group, *European Court of Justice May Invalidate Safe Harbor Framework*, Ballard Spahr LLP (Sept. 30, 2015), http://www.ballardspahr.com/alertspublications/legalalerts/2015-09-30-european-court-of-justice-may-invalidate-safe-harbor-framework.aspx.

102 James Ball, *NSA Prism Surveillance Program: How It Works and What It Can Do*, THE GUARDIAN (Jun. 8, 2013, 13:56), http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

stored and analyzed email and other communications that flowed across the internet.[103]

Critically, these NSA programs allegedly were authorized by law. To strengthen its counterterrorism efforts after the attacks of September 11, the United States had passed the USA PATRIOT ACT[104] in 2001 and the FISA Amendments Act of 2008 ("FAA").[105] The FAA created Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), establishing a framework for the bulk interception of foreign communications.[106]

The revealed practices of the NSA were met with widespread condemnation in the EU and depicted by critics as overreach by US security services.[107] To be sure, the EU had recognized the right of third countries to engage in national security surveillance, and had allowed exemptions from data protection legislation for such practices both in Europe and in the approved adequacy decisions, including the Safe Harbor framework. But, at the time, few if any policymakers imagined the enormity of the data collection apparatus revealed by the Snowden leaks. In March 2014, after a six-month review of the US national security framework, the European Parliament passed a resolution calling for the "immediate suspension" of transfers to the United States under Safe Harbor.[108]

2. Max Schrems Takes on Facebook

In the spring of 2011, Max Schrems was an Austrian law student on exchange at Santa Clara University School of Law.[109] During his time

---

[103] PCLOB Report, *supra* note 99, at 36.

[104] PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[105] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[106] *Id.*

[107] Hannah Allam & Jonathan S. Landay, *World's Anger at Obama Policies Goes Beyond Europe and the NSA*, MCCLATCHY DC (Oct. 25, 2013, 7:35 PM), http://www.mcclatchydc.com/news/nation-world/world/article24757900.html; Jedidiah Bracy, *Reactions to NSA Disclosures Continue*, INT'L ASS'N PRIVACY PROF'LS (June 10, 2013), https://iapp.org/news/a/Reactions-to-NSA-Disclosures-Continue.

[108] *US NSA: Stop Mass Surveillance Now or Face Consequences, MEPs Say*, European Parliament News (Mar. 12, 2014, 12:51 PM), http://www.europarl.europa.eu/news/en/news-room/20140307IPR38203/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say.

[109] Mary Ellen McIntire, *How a Law Seminar Inspired a Student to Bring a Case to Europe's Top Court*, The Chronicle of Higher Education (Oct. 7, 2015), http://chronicle.com/article/How-a-Law-Seminar-Inspired-a/233682.

at Santa Clara, Schrems attended a privacy law seminar featuring a lawyer from Facebook as the speaker. Schrems was "taken aback" when the lawyer explained that "they didn't take Europe's strict privacy laws very seriously, since companies rarely faced significant penalties for breaking them."[110] Schrems decided to write a term paper on the subject, and, upon return to Austria, he formed a non-profit, Europe versus Facebook, to challenge Facebook's privacy policies.[111] His organization filed more than twenty complaints against Facebook with the Irish Data Protection Commissioner ("DPC"), where Facebook's European operations are based.[112]

Two years later, just days after Snowden's revelations, Schrems filed another complaint with the DPC, asking it "to inquire if 'Facebook Inc' is forwarding my data to the NSA for compelling reasons of national security or if merely cooperating with the NSA voluntarily."[113] Furthermore, because Facebook used Safe Harbor to transfer data, Schrems challenged whether Safe Harbor's national security exemption was consistent with the Data Protection Directive and with the EU Charter of Fundamental Rights. Thus, Schrems asked the DPC "to review the validity of the 'Safe Harbor' [D]ecision."[114] Finding that the European Commission's Safe Harbor Decision precluded independent review of data transfers by national authorities, and that Schrems had presented no evidence that his own data had been accessed, the DPC refused to investigate the complaint.[115]

Schrems appealed the DPC's refusal to take action to the High Court of Ireland.[116] Schrems argued that the DPC "unlawfully fettered his own discretion" because "[i]t was irrational to rely upon [the Commission's Safe Harbor] Decision in circumstances where the Applicant's complaint is specifically contesting its validity and arises

---

[110] Robert Levine, *Behind the European Privacy Ruling That's Confounding Silicon Valley*, N.Y. TIMES, (Oct. 9, 2015), http://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html.

[111] *See* EUROPE VERSUS FACEBOOK, http://europe-v-facebook.org/EN/en.html (last visited Nov. 13, 2016).

[112] Levine, *supra* note 110.

[113] Schrems v. Data Protection Comm'r [2014] IEHC 310, Complaint against Facebook Ireland Ltd – 23 "PRISM" at 4, (Ir.), http://www.europe-v-facebook.org/prism/facebook.pdf.

[114] *Id.* at 6.

[115] Schrems v. Data Protection Comm'r [2014] IEHC 310, Statement of Opposition of the Respondent (Ir.), http://europe-v-facebook.org/JR_First_Response_DPC.pdf.

[116] Schrems v. Data Protection Comm'r [2014] IEHC 310, Application for Judicial Review (Ir.), http://europe-v-facebook.org/JR_Grounding_Documents.pdf.

from facts that were unknown or did not exist at the date of EU Commission Decision C2000/520/EC."[117] Therefore, he asked the court to order the DPC to investigate his complaint.[118]

The High Court first considered the question as a matter of Irish law.[119] Since "surveillance directly engages the constitutional right to privacy" as well as "the inviolability of the dwelling,"[120] if the question was controlled entirely by Irish law, the court found that "a significant issue would arise as to whether the United States 'ensures an adequate level of protection for the privacy and the fundamental rights and freedoms.'"[121] Recognizing, however, that Irish law was pre-empted by the European Commission's adequacy finding, pursuant to Article 25 of the Data Protection Directive, the court held that EU law must control.[122]

As a matter of EU law, the court noted that although the Safe Harbor Decision purported to prevent the DPC from investigating the complaint, two important developments had undermined its continued validity. First, the entry into force of the EU Charter required the European Commission to ensure that all data access, including by government authorities, was consistent with the EU Charter.[123] Second, "disclosures regarding mass and undifferentiated surveillance of personal data by the US security authorities, [and] the advent of social media" since the Commission decision in 2000 had undermined previous assumptions about the extent of US national security access.[124] Thus, pursuant to EU procedure, the court referred to the CJEU the question of whether, given these new legal and factual developments, the DPC was bound by the Commission's adequacy finding not to conduct its own independent investigation where an individual claims an interference with his EU Charter rights.[125]

---

[117] *Id.* at (E)(1).
[118] *Id.* at (D)(1–2).
[119] Schrems v. Data Protection Comm'r [2014] IEHC 310, Judgment (Ir.), http://www.europe-v-facebook.org/hcj.pdf.
[120] *Id.* ¶ 47.
[121] *Id.* ¶¶ 52, 56.
[122] *Id.* ¶ 57.
[123] *Id.* ¶ 65.
[124] *Id.* ¶ 67.
[125] *Id.* ¶ 71.

B. SCHREMS V. DATA PROTECTION COMMISSIONER

On September 23, 2015, after the CJEU heard arguments in *Maximilian Schrems v. Data Protection Commissioner* ("*Schrems*"), the Advocate General, Yves Bot, delivered his assessment of the case.[126] The Advocate General, a neutral party, found that "the existence of a decision adopted by the European Commission on the basis of Article 25(6) of Directive 95/46 does not have the effect of preventing a national supervisory authority from investigating a complaint alleging that a third country does not ensure an adequate level of protection of the personal data transferred and, where appropriate, from suspending the transfer of that data."[127] Two weeks later, the CJEU struck down the Safe Harbor Decision.[128]

The CJEU overturned the adequacy decision on two grounds. First, the Court held that the decision improperly limited the ability of DPAs to independently fulfill their mandates of protecting European citizens' data. Second, the Court determined that the Commission's decision failed to limit—or point to existing national law or international obligations that limit—the US government's ability to conduct indiscriminate surveillance.

1. The Role of Data Protection Authorities

In *Schrems*, the specific provision at issue was Article 3 of the Safe Harbor Decision.[129] Article 3 allowed a DPA to suspend data flows only when (a) the FTC has found that the US organization transferring data has violated the Principles of Safe Harbor, or (b) "there is a substantial likelihood that the Principles are being violated," as well as a reasonable basis for believing the FTC is not taking adequate steps, the transfer created an imminent risk of grave harm, and the DPA has made reasonable efforts to provide the organization with notice and an opportunity to respond.[130]

---

[126] Schrems v. Data Protection Comm'r [2014] IEHC 310, Judgment (Ir.), Opinion of Advocate General Bot.

[127] *Id.* ¶ 237.

[128] Schrems v. Data Protection Comm'r [2014] IEHC 310, Judgment (Ir.), http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.

[129] *Id.* ¶ 104.

[130] Safe Harbor Decision, *supra* note 79, at art. 3.

The CJEU first noted that "an essential component" of the Data Protection Directive's protections was its requirement for Member States "to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules."[131] The Data Protection Directive empowered DPAs with investigative authority, including "the power to collect all information necessary for the performance of their supervisory duties," as well as the authority to intervene by banning data transfers or engaging in legal proceedings.[132] This mandate, the Court explained, was further strengthened by Article 8 of the EU Charter, which guaranteed a right to the protection of personal data, under the control of an independent authority.[133]

Given the central role of DPA oversight to the rights enumerated in the Data Protection Directive and the EU Charter, the Court found that, "even if the Commission has adopted a[n adequacy] decision, . . . [DPAs] must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive."[134] Thus, the Court held Article 3 exceeded the Commission's authority by imposing limits upon the independent operation of DPAs.[135]

The Court established a process for individuals to challenge adequacy decisions before an appropriate DPA. DPAs must examine, "with all due diligence," any claim that data has been transferred to a country lacking adequate protections.[136] A DPA ruling must be appealable to a national court, which may refer the question to the CJEU if it finds that protections were inadequate.[137] Thus, in the case of Schrems's complaint, the Irish DPC was not entitled merely to rely on the Safe Harbor Decision to avoid investigating the complaint.

2. Limits to Surveillance

The CJEU next considered the Safe Harbor Decision's national security exemption.[138] If the national security exemption was read to contain no restrictions on government access, the Court found, then data

---

[131] Schrems [2014] IEHC 310, ¶¶ 40, 61.
[132] *Id.* ¶ 43.
[133] *Id.* ¶ 47.
[134] *Id.* ¶ 57.
[135] *Id.* ¶ 66.
[136] *Id.* ¶¶ 62–65.
[137] Schrems [2014] IEHC 310, ¶¶ 62–65.
[138] *Id.* ¶ 86.

transferred to a third country could be subjected to surveillance, "without any differentiation, limitation or exception . . . and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data."[139] Such "generalized" surveillance, the Court held, "must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the [EU] Charter."[140]

The Court, therefore, found that an "adequate level of protection" requires "the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights that is *essentially equivalent* to that guaranteed within the European Union."[141] While "the means to which that third country has recourse . . . may differ" from those in the EU, "those means must nevertheless prove, in practice, effective in order to ensure protection *essentially equivalent* to that guaranteed within the European Union."[142]

When determining the adequacy of protections in a third country, the Commission must consider "the content of the applicable rules in that country resulting from its domestic law and international commitments and the practice designed to ensure compliance with those rules."[143] The Commission also must "check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified,"[144] taking into account "the circumstances that have arisen after the decision's adoption."[145] Thus, review of the third country's protections "should be strict."[146]

Importantly, the Court did not consider the substance of US surveillance law. Rather it assessed only the European Commission's process for determining adequacy, which lacked any substantive review of US surveillance law.[147] Under this review, the Safe Harbor Decision fell because it did not itself consider the equivalency of national security legislation, leaving a loophole, which according to Snowden and Schrems, was in fact used extensively to access European data without

---

[139] *Id*. ¶ 93.
[140] *Id*. ¶ 94.
[141] *Id*. ¶ 73 (emphasis added).
[142] *Id*. ¶ 74 (emphasis added).
[143] Schrems [2014] IEHC 310, ¶ 75.
[144] *Id.* ¶ 76.
[145] *Id.* ¶ 77.
[146] *Id.* ¶ 78.
[147] *Id.* ¶ 98.

due safeguards.[148] Without assessing either the national security protections offered in the United States or those offered by EU Member States, the Court made clear that any future adequacy decision would have to account for national security access.

C. MEASURING ADEQUACY: ESSENTIALLY EQUIVALENT TO WHAT?

In *Schrems*, the CJEU held that "the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter."[149] Since the Court did not consider the limits to US government access, however, it did not delineate the precise contours of those EU Charter rights.

A debate has since erupted over the proper application of the "essentially equivalent" test. While the concept of equivalency requires a comparison of the third country's protections from surveillance to those offered in the EU, it is not clear what exactly those EU protections are. It is, therefore, necessary to define the scope of comparison.

On the one hand, according to Article 4(2) of the Treaty on European Union ("TEU"), national security falls outside the scope of EU law and is left exclusively to the Member States.[150] Thus, it might be appropriate to ground a comparison of a third country's laws to the practices of EU Member States since the EU itself is not competent to legislate in this area.[151] Alas, Member State law spans a broad spectrum, so it would be difficult to elucidate a uniform standard to ground the comparison to a third country's law.[152] These surveys suggest, moreover,

---

[148] *Id.* ¶ 88.

[149] Schrems [2014] IEHC 310, ¶ 73.

[150] "The Union shall respect the equality of Member States before the Treaties as well as . . . their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. *In particular, national security remains the sole responsibility of each Member State.*" Treaty on European Union, art. 4(2), Feb. 7, 1992, 1992 O.J. (C 191) 1 (emphasis added).

[151] Jacques Bourgeois et al., Sidley Austin LLP, Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States 22-23 (Jan. 25, 2016), http://www.sidley.com/~/media/publications/essentially-equivalent—-final.pdf.

[152] For a comparison of Member State surveillance laws, see European Union Agency for Fundamental Rights, Surveillance By Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU 18-27, (2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf. *See also* European Parliament Directorate-General for

that there is a gap between the practices of some Member States and the principles articulated in the *Schrems* judgment, ostensibly meaning that when it comes to government access, even the data protection standard in the EU is "inadequate."[153]

On the other hand, "[t]he territorial scope of the [EU] Charter is the same as that of EU law."[154] Thus, the EU Charter may serve as the appropriate baseline because the Commission's adequacy assessment is governed by the Data Protection Directive, an EU-level law.[155] The Commission, therefore, must assess adequacy "in the light of the Charter."[156] As a matter of realpolitik, to focus on the shortcomings of Member State protections is "pointless . . . since this is irrelevant for the standard of protection articulated by the Court. A violation of fundamental rights by a third country cannot be excused because EU [Member State] standards themselves may be lacking."[157]

For the sake of analysis below, this article adopts the second approach, which is stricter. If a third country's law passes muster under this interpretation, it would *a fortiori* satisfy the lower bar set by Member State law. Although Member State legislation may provide helpful case studies to test the EU Charter's protections, to survive a challenge before the CJEU and provide confidence in ongoing transfers, Canada's adequacy decision must meet the EU Charter standard.

Internal Policies, Parliamentary Oversight of Security and Intelligence Agencies in the European Union (2011), http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf.

[153] Hannah Kuchler & Duncan Robinson, *Top Lawyer Claims US Does Better on Data Protection Than EU*, FINANCIAL TIMES (Jan. 25, 2016), http://www.ft.com/intl/cms/s/0/b5287afc-c297-11e5-808f-8231cd71622e.html; *see also* Nils Muiznieks, *Europe Is Spying on You*, N.Y. TIMES (Oct. 27, 2015), http://www.nytimes.com/2015/10/28/opinion/europe-is-spying-on-you-mass-surveillance.html ("Many of the surveillance policies that have recently been adopted in Europe fail to abide by [ECtHR] legal standards. Worse, many of the new intrusive measures would be applied without any prior judicial review establishing their legality, proportionality or necessity.").

[154] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post* Schrems 15 (Univ. of Cambridge Faculty of Law Research Paper No. 14/2016), http://ssrn.com/abstract=2732346.

[155] *Id.*

[156] Schrems [2014] IEHC 310, ¶ 73.

[157] Kuner, *supra* note 154, at 14–16.

1. Interpretation of the EU Charter is Informed by the Jurisprudence of the European Court of Human Rights

In parallel to the EU Charter protections, the European Convention on Human Rights ("ECHR") extends human rights protections to all individuals in signatory nations, which include all of the EU Member States, and is enforced by the European Court of Human Rights ("ECtHR").[158] Although not binding on the CJEU, Article 8 of the ECHR contains a "right to respect for private and family life," which mirrors the EU Charter's Article 7 protections.[159]

To the extent that the rights of the ECHR and the EU Charter overlap, the EU Charter provides, "the meaning and scope of those rights shall be the same as those laid down by the said Convention."[160] Thus, the CJEU occasionally has turned to ECtHR jurisprudence in defining the EU Charter's protections. For example, in *Digital Rights Ireland*, the CJEU quotes from several ECtHR cases in defining the appropriate standard for privacy protections under the EU Charter.[161]

In contrast to the CJEU, whose national security jurisprudence is sparse, the ECtHR has a long track record of balancing national security interests against the privacy rights of individuals. Thus, like the Article 29 Working Party162 and the European Commission itself,[163] this article

---

[158] Convention for the Protection of Human Rights and Fundamental Freedoms, 213 U.N.T.S. 222 (Nov. 4, 1950) [hereinafter ECHR].

[159] "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security . . . ." *Id.*, art. 8.

[160] EU Charter, *supra* note 22, art. 52(3).

[161] *See* Digital Rights Ireland, *supra* note 26, ¶ 35. ("Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., Leander v. Sweden, 26 March 1987, § 48, Series A no 116; Rotaru v. Romania [GC], no. 28341/95, § 46, ECHR 2000-V; and Weber and Saravia v. Germany (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.").

[162] Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision* WP 238 (2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[163] *See* Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C(2016) 4176, [hereinafter Privacy Shield Decision], http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (citing cases from the ECtHR for reference).

will turn to the jurisprudence of the ECtHR with respect to national security surveillance to help inform the EU Charter standard.

2. Privacy Shield as the New Standard for Adequacy?

Following the Snowden disclosures, the European Commission issued thirteen recommendations for "restoring trust in EU-U.S. data flows,"[164] which set off a round of negotiations between EU and US officials on strengthening the Safe Harbor framework.[165] On February 2, 2016, almost four months after *Schrems* invalidated Safe Harbor, the European Commission and the US Department of Commerce announced they had reached an agreement on the "EU-US Privacy Shield," a rebranded replacement for Safe Harbor.[166] A draft adequacy decision and supporting documentation were released on February 29, 2016,[167] and the Article 29 Working Party issued its assessment on April 13, finding that Privacy Shield did not fully address all the issues in the *Schrems* decision.[168] After revising the agreement to address these concerns, however, the European Commission officially approved the Privacy Shield package on July 12, 2016.[169] As the latest and most high-profile statement on international data transfers, Privacy Shield may come to define the standard for future adequacy decisions, or at least inform the negotiation of future adequacy decisions before the European Commission.

---

[164] European Commission Press Release IP/13/1059, Restoring Trust in EU-US Data Flows – Frequently Asked Questions (Nov. 27, 2013), http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

[165] Stephen Gardner, *EU Cites U.S. Data Transfer Pact Progress Amid Privacy Regulation Reform Negotiations*, BLOOMBERG BNA (June 9, 2014), http://www.bna.com/eu-cites-us-n17179891134/.

[166] European Commission Press Release IP/16/216, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm

[167] European Commission Press Release IP/16/433, Restoring Trust in Transatlantic Data Flows Through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield (Feb. 29, 2016), http://europa.eu/rapid/press-release_IP-16-433_en.htm.

[168] *See* Data Protection Working Party, *supra* note 162, at 4 (finding that the Privacy Shield does not fully exclude the possibility of massive and indiscriminate collection of personal data by U.S. authorities and that the Ombudsperson mechanism "is not sufficiently independent and is not vested with adequate powers to effectively exercise its duty and does not guarantee a satisfactory remedy in case of disagreement.").

[169] European Commission Press Release IP/16/2461, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016).

Spanning more than 130 pages, including supporting materials provided by high-level US officials, Privacy Shield is clearly different from previous adequacy decisions.[170] It included statements and commitments from the Department of Commerce, Secretary of State, Federal Trade Commission, Secretary of Transportation, Office of the Director of National Intelligence ("ODNI"), and Department of Justice.[171] It also heightened the requirements on organizations that certify to its principles.[172] A notable similarity, however, is that Privacy Shield maintained Safe Harbor's system of self-certification.

The Privacy Shield adequacy decision detailed the limits to national security access that exist in US law, including some of the changes that were implemented since 2013.[173] One important legislative development was the passage of the USA FREEDOM Act,[174] which placed new limits on the NSA's bulk telephony metadata program, introduced reforms to FISA Court oversight, and imposed new transparency and reporting requirements associated with government data collection.[175] The Judicial Redress Act extended the protections of the US Privacy Act of 1974 to non-US residents, including the ability to bring civil claims against US agencies.[176] Most significantly, Presidential Policy Directive 28, which was executed in response to the Snowden disclosures and binds all federal executive agencies, limited bulk foreign surveillance to only six specific purposes.[177]

---

[170] The Canadian adequacy decision, by contrast, is scarcely four pages. *See* Commission Decision 2002/2/EC, *supra* note 53.

[171] ANNEXES to the Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C(2016) 4176, [hereinafter Privacy Shield Annexes], http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf.

[172] Gabe Maldoff, *We Read Privacy Shield so You Don't Have to*, INT'L ASS'N PRIVACY PROF'LS (Mar. 7, 2016), https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to/.

[173] Privacy Shield Decision, *supra* note 163.

[174] USA FREEDOM Act, Pub.L. No. 114-23, 129 Stat. 268 (2015).

[175] Arielle Brown, *The USA FREEDOM Act Explained*, INT'L ASS'N PRIVACY PROF'LS (June 16, 2015), https://iapp.org/news/a/the-usa-freedom-act-explained/.

[176] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282. Note, however, that redress for violations related to national security access is specifically exempt. *Id.*

[177] *See* Press Release, White House Office of the Press Secretary, Presidential Policy Directive: Signals Intelligence Activities (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

> (In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data . . . only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to

As a result of the Privacy Shield negotiations, the US State Department agreed to appoint an ombudsperson with responsibility for investigating complaints by EU residents, even if they cannot demonstrate that their data has in fact been accessed.[178] Additionally, in supporting letters, high-level US officials provided explicit assurances on the limits of national security access to EU data. For example, ODNI stated that the US Intelligence Community "does not engage in indiscriminate surveillance of anyone, including ordinary European citizens," and that US limitations on access would apply to any interception of communications outside the United States, such as in transit on transatlantic cables.[179] It is not clear to what extent these assurances denote new limits on surveillance, or whether they repeat existing policy and are designed to assure the European public. If they do supply new limits, some have questioned whether they will have binding effect on future administrations.[180] Regardless of any criticism, however, these letters could raise the bar for future adequacy decisions, which will perhaps have to include similar assurances.

3. Crafting a Standard

Whatever the case was pre-*Schrems*, post-*Schrems* adequacy decisions will have to compare foreign regimes to the standard set out in the EU Charter. Although in *Schrems* the CJEU did not evaluate US national security access, it made clear that the EU Charter prohibits mass and indiscriminate surveillance.

In pointing to the failures of the Safe Harbor Decision, the *Schrems* Court enunciated broad principles that could inform the essential equivalence test required by the EU Charter. The Court found

---

> the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section. In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified in this section.).

[178] Privacy Shield Annexes, *supra* note 171.

[179] *Id.*

[180] Angelique Carson, *How Sturdy is the Privacy Shield?*, INT'L ASS'N PRIVACY PROF'LS (Feb. 3, 2016), https://iapp.org/news/a/how-sturdy-is-the-privacy-shield/.

that, where legislation interferes with the EU Charter, it must "lay down clear and precise rules . . . so that the persons whose personal data is concerned have sufficient guarantees . . . against the risk of abuse and against any unlawful access and use of that data."[181] The Court also noted that Safe Harbor may have permitted US authorities to access data "beyond what was strictly necessary and proportionate to the protection of national security" and without providing EU residents "administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased."[182] Similarly, in *Digital Rights Ireland*, the Court found, "the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[183]

Summarizing these principles, the Article 29 Working Party articulated the *essentially equivalent* test as follows:

> (1) processing must be based on clear, precise, and accessible rules so that a reasonably informed person can foresee what might happen with her data when transferred ("clear, precise, and accessible rules");
>
> (2) government access to personal data must be strictly necessary and proportionate to the protection of national security ("strictly necessary and proportionate");
>
> (3) there must be a mechanism of independent oversight of national security access that is effective and impartial ("independent oversight"); and,
>
> (4) adversely affected individuals must have access to effective judicial or administrative redress before an independent body ("effective redress").[184]

In sum, the test for essential equivalence under the EU Charter, as enunciated in *Schrems*, requires a third country to meet the four

---

[181] Schrems [2014] IEHC 310, ¶ 91.

[182] *Id.* ¶ 90.

[183] Digital Rights Ireland, *supra* note 26, ¶ 38.

[184] *See* Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment (Feb. 3, 2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

guarantees outlined by the Article 29 Working Party. Because the Court has never evaluated a third country under this test, and because the ECHR contains a right to privacy similar to that in the EU Charter, the case law of the ECtHR helps to inform the application of this test. Additionally, as the first regime specifically designed to address the concerns in *Schrems*, Privacy Shield may further elaborate the appropriate application of the test.

V. CANADIAN NATIONAL SECURITY SAFEGUARDS

This section reviews Canada's national security framework. It first outlines the mandates and powers of the agencies most involved in national security before reviewing the limits of their authority. The review centers on the four-part test above in addition to highlighting how the Canadian protections compare to the key commitments the EU obtained from the United States in Privacy Shield.

Canadian national security and intelligence gathering activities are primarily the responsibility of three federal agencies: the Royal Canadian Mounted Police ("RCMP"), the Canadian Security Intelligence Services ("CSIS"), and the Communications Security Establishment ("CSE"). With few exceptions, each agency is governed by a separate statutory framework. The following sections outline each agency's legal authority to conduct foreign surveillance as well as the agencies' ability to share data amongst themselves and with foreign partners.

A. THE ROYAL CANADIAN MOUNTED POLICE ("RCMP")

Canada's federal law enforcement agency, the RCMP, is intimately involved in national security investigations and communications surveillance.[185] Its mandate to investigate terrorism-related offenses arises under a number of acts, including the Security Offences Act,[186] the Security of Information Act,[187] the Anti-Terrorism Act,[188] as well as the Criminal Code of Canada.[189] These acts provide the

---

[185] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar: Analysis and Recommendations (2006), http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/AR_English.pdf [hereinafter Arar Commission].

[186] Security Offences Act, R.S.C. 1985, c S-7 (Can.).

[187] Security of Information Act, R.S.C. 1985, c O-5 (Can.).

[188] Anti-Terrorism Act, S.C. 2001, c. 41 (Can.).

RCMP with the authority to investigate "[a]ctivities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state" as well as terrorist financing, espionage or clandestine foreign-influenced activities directed at Canada's interests.[190] In pursuit of these mandates, the RCMP has repeatedly called for expanding its legal authority to gather intelligence.[191]

Canadian law distinguishes between *interception* of communications and lawful *access to stored* information, with each subject to a distinct legal framework. The interception framework applies when the RCMP "listen[s] to, record[s] or acquire[s] a communication or acquire[s] the substance, meaning or purport thereof."[192] As interpreted by a plurality of the Supreme Court in *R. v. Telus Communications*, the RCMP must apply the interception framework when seeking the "the *prospective* production of *future* [communications]," as opposed to accessing already-stored communications and records.[193]

The Criminal Code of Canada makes it a crime for anyone, including public authorities, to "wilfully intercept[] a private communication," unless the interception is authorized by an enumerated exception.[194] The most important exception to this prohibition allows police officers to intercept a communication with authorization from a judge.[195] Interception authorizations are subject to a higher standard than ordinary search warrants.[196] In order to obtain an authorization, the police must show "reasonable and probable grounds" to believe that interception will provide evidence of an offense and "that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed, or the urgency of the matter is such that it would be impractical to carry out the investigation

---

[189] *The RCMP and Canada's National Security*, ROYAL CANADIAN MOUNTED POLICE, http://www.rcmp-grc.gc.ca/nsci-ecsn/nsci-ecsn-eng.htm (last modified Jan. 14, 2016).

[190] *Id.*

[191] Ian Mulgrew, *Too Much Rhetoric in Calls for Expanded Police, Surveillance Powers*, VANCOUVER SUN (Oct. 28, 2014), http://www.vancouversun.com/news/mulgrew+much+rhetoric+calls+expanded+police+surveillance+powers/10336299/story.html.

[192] Criminal Code of Canada, R.S.C. 1985, c C-46, s. 183.

[193] R. v. TELUS Commc'n., [2013] 2 S.C.R. 3 (Can.).

[194] Criminal Code, *supra* note 192, § 184(1).

[195] *Id.* § 184(2)(b).

[196] *Id.* § 487.

of the offence using only other investigative procedures."[197] In other words, in many circumstances, police must show "investigative necessity" to conduct a wiretap.[198] Only judges of the Superior Court may authorize such interceptions. They may do so only in the investigation of specific designated offenses and with the written consent of the Minister of Public Safety or the Attorney General.[199] Interception may extend up to sixty days[200] and the target must be provided notice within ninety days after the interception.[201]

Investigations of "criminal organizations and terrorism offences" are subject to less onerous standards.[202] First, the police do not need to prove investigative necessity to secure judicial authorization—the ordinary reasonable and probable grounds standard is sufficient.[203] Second, for these offenses, the maximum period of interception may extend up to one year.[204] Finally, while ordinarily the target must be notified within ninety days of an interception unless the investigation is "continuing,"[205] for terrorism and criminal organizations investigations, a judge may extend the notification period up to three years, even if the investigation is no longer ongoing.[206]

The acquisition of stored communications and records, such as the text of an email or a recorded message, is subject to the lower warrant standards used for ordinary searches and seizures set out in the provisions of Part XV of the Criminal Code.[207] Unlike the interception framework, for stored communications and records, the police need not demonstrate investigative necessity and may seek authorization from provincially-appointed judges—not just from Superior Court judges.[208]

Part XV allows a provincial or federal court judge to authorize the RCMP to access "a document or data" with a "general production

---

[197] *Id.* § 186(1)(b).

[198] Steven Penney, National Security Surveillance in an Age of Terror: Statutory Powers and Charter Limits, 48 OSGOODE HALL L.J. 247, 256 (2010).

[199] Criminal Code, *supra* note 192, at § 185(1).

[200] *Id.* § 184.2(4)(e).

[201] *Id.* § 196.1(1).

[202] *Id.* § 186(1.1).

[203] *Id.*

[204] *Id.* § 186.1.

[205] Criminal Code, *supra* note 192, § 196.1(3).

[206] *Id.* § 196.1(5).

[207] Steven Penney, Updating Canada's Communications Surveillance Laws: Privacy in the Digital Age, 12 CAN. CRIM. L. REV. 115, 126–29 (2008).

[208] Criminal Code, *supra* note 192, § 552.

order"[209] or to "use any device or investigative technique or procedure" under a "general warrant."[210] To obtain a general warrant or production order, the RCMP must demonstrate that it has "reasonable grounds to believe" that a crime has been or will be committed and that the search will reveal evidence of the crime.[211]

Part XV provides a separate standard for access requests to tracking data[212] and transmission data.[213] These pieces of information, commonly labelled "metadata," relate to the location of a transaction, individual or thing, or to "the telecommunications functions of dialling, routing, addressing or signalling."[214] Unlike under a general warrant, in order to obtain a warrant for access to metadata, the RCMP must satisfy only the lower standard of "reasonable grounds to suspect" or "reasonable suspicion."[215]

B. THE CANADIAN SECURITY INTELLIGENCE SERVICES ("CSIS")

CSIS is a civilian intelligence agency that was established in 1984 and lies within the authority of the Minister for Public Safety.[216] The CSIS Act provides the agency with two distinct mandates: Section 12 and Section 16. Under its Section 12 authority, CSIS is authorized to collect and analyze intelligence related to "threats to the security of Canada."[217] These threats include espionage or sabotage, clandestine or deceptive foreign influenced activities that are detrimental to Canadian interests, threats or acts of serious violence for achieving political, religious, or ideological objectives, and activities aimed at the unlawful destruction or overthrow of the Canadian government.[218] Lawful advocacy, protest, and dissent, however, are specifically exempt.[219]

---

[209] *Id.* § 487.014(1).

[210] *Id.* § 487.01(1).

[211] *Id.* §§ 487.01(1)(a), 487.014(2).

[212] *Id.* § 487.017(1).

[213] *Id.* § 487.016(1).

[214] Criminal Code, *supra* note 192, § 487.011.

[215] *See* R. v. Kang-Brown, [2008] 1 S.C.R. 456, para. 164 (Can.) ("In my view, 'reasonable grounds to suspect' is substantively equivalent to 'reasonable suspicion.' It is clear that the standard . . . is lower than that of 'reasonable grounds to believe[.]'").

[216] Canadian Security Intelligence Service Act, R.S.C. 1985, c C-23 (Can.) [hereinafter CSIS Act].

[217] *Id.* § 12(1).

[218] *Id.* § 2 ("*threats to the security of Canada* means (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage, (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any

Under Section 12 of the CSIS Act, CSIS may collect information, either through interception or by accessing stored records, only "to the extent that it is strictly necessary" for its mandate.[220] It is permitted to retain and analyze such information if it relates to "activities that may on reasonable grounds be suspected of constituting threats to the security of Canada."[221] CSIS's inspector general has described this standard as "demonstrable grounds for suspicion," with the burden on CSIS to document those grounds.[222] Notably, CSIS may investigate threats to the security of Canada either "within or outside Canada."[223]

CSIS's second mandate, Section 16 of the CSIS Act, allows the agency to collect "information or intelligence relating to the capabilities, intentions or activities" of any foreign state or any person other than a Canadian citizen, permanent resident or Canadian corporation.[224] CSIS may act under Section 16 only to provide assistance to the Minister of National Defence or the Minister of Foreign Affairs, and the relevant minister must, therefore, provide "personal consent in writing."[225] Unlike Section 12, under this mandate, CSIS may collect information or intelligence only "within Canada."[226] Thus, while Section 12 is focused on "threats to the security of Canada," at home or abroad, Section 16 provides CSIS broader foreign intelligence-gathering authority within Canada, "in relation to the defence of Canada or the conduct of the international affairs."[227]

Under both mandates, where the CSIS Director or another qualified employee "believes, on reasonable grounds, that a warrant

---

person, (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada, but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).").

[219] *Id.*

[220] *Id.* § 12(1).

[221] *Id.*

[222] Craig Forcese, *Assessing CSIS: 2. Scope and Mandate*, THE NATIONAL SECURITY BLOG (Jan. 16, 2012), http://craigforcese.squarespace.com/national-security-law-blog/2012/1/16/assessing-csis-2-scope-and-mandate.html.

[223] CSIS Act, *supra* note 216, § 12(2).

[224] *Id.* § 16(1).

[225] *Id.* § 16(3)(b).

[226] *Id.* § 16(1).

[227] *Id.*

under this section is required,"[228] he or she may petition a judge for a warrant "to intercept any communication or obtain any information, record, document or thing."[229] Thus, the CSIS Act applies the same standard for intercepting private communications as it does to accessing stored communications. In executing a judicial warrant, CSIS may "enter any place or open or obtain access to any thing[,] search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or[,] install, maintain or remove any thing."[230]

To obtain a warrant, CSIS must supply the judge with a statement of approval from the Minister of Public Safety,[231] an elected member of the Cabinet. In the case of Section 16 warrants, the warrant application also must include the written request of either the Minister of National Defence or Foreign Affairs.[232] The warrant must state the type of communication or information sought, the persons or classes of persons who will execute the warrant, the identity of the target of the investigation, if known, and the period of time for which the warrant will be in force.[233] CSIS warrants may last for up to one year[234] and there is no requirement to inform the targets or parliament of the warrant after the fact. Importantly, the CSIS Act requires CSIS to demonstrate investigative necessity to obtain a warrant.[235]

The CSIS Act also established the Security Intelligence Review Committee ("SIRC") to oversee and review CSIS activities.[236] Members of SIRC are selected from the Privy Council by the Prime Minister in consultation with the Leader of the Opposition and the House of

---

[228] *Id.* § 21(1).

[229] CSIS Act, *supra* note 216, § 21(3).

[230] *Id.*

[231] *Id.* § 21(1).

[232] *Id.* § 16(3)(a).

[233] *Id.* § 21(4).

[234] However, where the warrant is designed to investigate "activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada," it may only extend up to a maximum of 60 days. *Id.* § 21(5).

[235] *See* CSIS Act, *supra* note 216, § 21(2)(b) (a warrant may be issued only if "other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (a) would not be obtained.").

[236] *Id.* § 34(1).

Commons.[237] SIRC must review directives of the Minister to the agency, including directives under Section 16.[238] Additionally, SIRC is required to investigate complaints against CSIS by "any person" if the person has lodged a complaint with the Director of CSIS and he or she failed to timely respond or if SIRC is satisfied that the complaint is "not trivial, frivolous, vexatious or made in bad faith."[239] It also must produce an annual report to the Minister and Parliament, which must include a record of the number of warrants that were issued in that year.[240]

C. THE COMMUNICATIONS SECURITY ESTABLISHMENT ("CSE")

Canada's foreign surveillance arm, the Communications Security Establishment (CSE), is a civilian unit of the Department of National Defence.[241] It was created, prior to the Second World War, to collect signals intelligence, which includes acquiring and processing foreign electronic communications to advance the nation's interests in defense, security and international relations.[242] CSE has three specific mandates: (a) "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;" (b) to advise the government on ensuring the protection of electronic information and infrastructure; and, (c) "to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."[243] Under the third mandate, CSE is "subject to any limitations imposed by law on federal law enforcement and security agencies in the performance of their duties."[244]

CSE's mandate to conduct surveillance targeted at non-Canadian citizens abroad is subject to fewer limitations than that of CSIS. CSE is

---

[237] *Id.*

[238] *Id.* § 38(1).

[239] *Id.* § 41(1).

[240] *Id.* § 53(1),(2).

[241] Martin Rudner, Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism, 22 INTEL. AND NAT'L SEC. 473, 474 (2007). Martin Rudner, Canada's Communications Security Establishment: From Cold War to Globalisation, CENTRE FOR SECURITY AND DEFENCE STUDIES, CARLETON UNIVERSITY, Occasional Paper No. 22, 7 (2000), available at http://circ.jmellon.com/docs/pdf/canadas_communications_security_establishment_from_cold_war_to_globalization.pdf

[242] Rudner, *From Cold War to Globalisation*, *supra* note 241, at 6–12.

[243] National Defence Act, R.S.C. 1985, c N-5, s. 273.64(1) (Can.).

[244] *Id.* § 273.64(3).

not required to obtain a judicial warrant to intercept private communications.[245] Instead, CSE must obtain authorization from the Minister of National Defense in writing. The minister may authorize the interception of private communications "in relation to an activity or class of activities specified in the authorization" if:

> (a) the interception will be directed at foreign entities located outside Canada; (b) the information to be obtained could not reasonably be obtained by other means;
>
> (c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
>
> (d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.[246]

The Office of the CSE Commissioner, an independent review agency, is tasked with ensuring CSE acts in compliance with the law and it may undertake investigations in response to a complaint from any person.[247] The CSE Commissioner must be a retired or supernumerary Superior Court judge[248] and he must deliver a report to Parliament each year on his findings.[249]

D. DATA RETENTION AND INFORMATION SHARING

The Privacy Act of Canada, which regulates the government's collection and use of personal information, states that data used "for an administrative purpose" must be retained for a period of time that gives a person "a reasonable opportunity to obtain access to the information."[250] The data must then be disposed "in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister" with regards to the specific government agency in question.[251] Certain databases may be exempt[252] from these requirements where the

---

[245] *Id.* § 273.65(1).
[246] *Id.* § 273.65(2).
[247] *Id.* § 273.63(2).
[248] *Id.* § 273.63(1).
[249] National Defence Act, *supra* note 243, § 273.63(3).
[250] Privacy Act, *supra* note 34, § 6(1).
[251] *Id.* § 6(3).
[252] *Id.* § 18(1).

information in the databases relate predominantly to "international affairs and defence"[253] or "law enforcement and investigation."[254]

The databases of the RCMP, CSIS, and CSE that relate to foreign intelligence are designated as exempt banks under the law.[255] Nonetheless, both the RCMP and CSIS have published their guidelines for data retention, which are publicly accessible on their respective websites.[256] CSE, by contrast, does not disclose its retention policies.[257] Under the Security of Information Act, an agency is prohibited from disclosing secret information to any other person, including other government agencies, unless specifically authorized under the agency's mandate.[258]

In 2015, in response to terrorist attacks in Ottawa and Saint-Jean-sur-Richelieu, Quebec, Canada passed a controversial security law, Bill C-51, aimed at increasing the government's anti-terror powers.[259] The law, which provided CSIS greater authority to disrupt potential threats and gave the RCMP more leeway when making preventive arrests, also contained the Security of Information Sharing Act ("SCISA"). Designed to facilitate information sharing among federal agencies, SCISA permitted any federal agency to share information with any of seventeen other federal agencies, including all three discussed above, if the information is "relevant" to "activities that undermine the security of Canada."[260]

---

[253] *Id.* § 21.

[254] *Id.* § 22.

[255] Privacy Comm'r of Can., Audit Report of the Privacy Commissioner of Canada: Examination of RCMP Exempt Data Banks, Section 36 of the *Privacy Act* (Feb. 2008), https://www.priv.gc.ca/media/1203/rcmp_080213_e.pdf.

[256] *See* Personal Information Banks, ROYAL CANADIAN MOUNTED POLICE, http://www.rcmp-grc.gc.ca/atip-aiprp/infosource/pib-frp-eng.htm#ppu025 ("Information in this bank is retained by the RCMP for a minimum of two years. If the file has been designated as having enduring value it will be transferred to the control of Library and Archives Canada, otherwise it will be retained by the RCMP until it no longer has business value. At that point, it will be destroyed."). *See also* Sources of Federal Government and Employee Information, CANADIAN SEC'Y INTELLIGENCE SERV., https://www.csis.gc.ca/tp/nfsrc-en.php (last modified Sept. 22, 2016) (setting different retention periods for different categories of data).

[257] Colin Freeze, *CSEC Won't Say How Long it Keeps Canadians' Private Data*, THE GLOBE AND MAIL (Aug. 04, 2014, 9:20 PM), http://www.theglobeandmail.com/news/national/csec-wont-say-how-long-it-keeps-canadians-private-data/article19910556/.

[258] Security of Information Act, R.S.C. 1985, c. O-5 (Can.).

[259] Daniel Leblanc & Chris Hannay, *Privacy, Security and Terrorism: Everything You Need to Know About Bill C-51*, THE GLOBE AND MAIL (Mar. 10, 2015, 10:43 AM), http://www.theglobeandmail.com/news/politics/privacy-security-and-terrorism-everything-you-need-to-know-about-bill-c-51/article23383976/.

[260] Security of Canada Information Sharing Act, S.C. 2015, c 20, § 5(1) (Can.) [hereinafter SCISA].

1. Analysis of Canadian Safeguards

The 2001 European Commission decision awarding Canada adequacy status did not contemplate any review of national security access. Thus, this article is not a re-examination, but rather a first examination of this body of Canadian law under not just the newly articulated adequacy standard, but under any standard for adequacy.

This section compares Canada's laws on foreign surveillance against the EU Charter protections, as set forth in *Schrems*, using the four-prong test articulated by the Article 29 Working Party. Specifically, this section assesses whether (a) Canadian law provides clear, precise and accessible rules, (b) those rules restrict access only to what is strictly necessary and proportionate, (c) there is sufficiently independent oversight, and (d) Europeans have access to effective redress mechanisms in Canada.

E. CLEAR, PRECISE, AND ACCESSIBLE RULES

In *Schrems*, the CJEU held that a country may interfere with a fundamental right only when provided by law, under clear, precise and accessible rules that impose certain minimum safeguards.[261] The law must establish "an objective criterion . . . by which to determine the limits of the access by public authorities."[262] Under case law from the ECtHR, national security laws must provide a level of foreseeability such that individuals have an adequate indication of the circumstances and conditions that might trigger an interference with a fundamental right. In *Roman Zakharov v. Russia*, the ECtHR held that, in the context of secret surveillance, however, "'foreseeability' of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance."[263] Any discretion accorded to public authorities must, nonetheless, be constrained "with sufficient clarity to give the individual adequate protection against arbitrary interference."[264]

---

[261] Schrems [2014] IEHC 310, ¶ 91.

[262] *Id.* ¶ 93.

[263] Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R. ¶ 247 (2015), http://hudoc.echr.coe.int/eng?i=001-159324.

[264] Weber & Saravia v. Germany, App. No. 54934/00, ¶¶ 93–94, (2006), http://hudoc.echr.coe.int/eng?i=001-76586.

Much like in the United States, Canadian surveillance law is not secret. It is encoded by statute, in the Criminal Code of Canada,[265] the National Defence Act,[266] and the Canadian Security Intelligence Service Act,[267] all of which are accessible to the general public within and outside of Canada. These statutes outline, with a high level of specificity, the contours of the legal authority available to public authorities for national security surveillance. However, (and this too is similar to the United States), significant interpretive ambiguities undermine the clarity of the legislative mandate, particularly surrounding (i) the application of constitutional protections to foreigners, (ii) the definition of "private communications," and (iii) opaque information sharing practices among Canada and its allies.

1. The Application of the Canadian Charter of Rights and Freedoms to Foreign Searches is Unsettled

The Canadian Charter of Rights and Freedoms ("Canadian Charter") guarantees, under Section 8, "the right to be secure against unreasonable search or seizure."[268] This right protects "at least" a person's "'reasonable' expectation of privacy,"[269] which is implicated whenever a search reveals a person's "biological core."[270] It forms a fundamental backstop against unreasonable surveillance measures and, therefore, underlies and reinforces the statutory structure to set limits to government access.

Although the "reasonable expectation of privacy" concept is reflected in the Criminal Code's definition of "private communications," the Canadian Charter also offers protections in situations not covered by statute. In *R. v. Spencer*,[271] the Supreme Court of Canada confronted a

---

[265] Criminal Code, *supra* note 192.

[266] National Defence Act, *supra* note 243.

[267] CSIS Act, *supra* note 216.

[268] Canadian Charter, *supra* note 31, § 8.

[269] Hunter v. Southam Inc., [1984] 2 S.C.R. 145, 159 (Can.).

[270] *See* R. v. Plant, [1993] S.C.R. 281 (Can.), http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1049/index.do ("In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.").

[271] R. v. Spencer, [2014] 2 S.C.R. 212 (Can.), https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do.

challenge to a company's voluntary disclosure of a customer's information to the government. Recall that PIPEDA prohibits a Canadian company that holds personal information from disclosing it to third parties without consent. PIPEDA provides an explicit exception, however, for disclosures made to a government institution that has "identified its lawful authority."[272] In that case, the government asked an internet service provider to link an IP address to a user's name and account information, relying on a section of the Criminal Code that allows a public officer to "ask a person to voluntarily . . . provide a document to the officer that the person is not prohibited by law from disclosing."[273]

Recognizing that a user has a "right to anonymity" under Section 8 that applies even in public places, the Supreme Court held that "it would be reasonable for an Internet user to expect that a simple request by police would not trigger an obligation to disclose personal information or defeat PIPEDA's general prohibition on the disclosure of personal information without consent."[274] Thus, the Court held that the service provider was not permitted to disclose personal information to the government upon a voluntary request for assistance.[275] Instead, the government was required to present a judicial warrant.

The *Spencer* ruling goes far toward ensuring that the government access framework cannot easily be circumvented through "voluntary" requests for cooperation. It also demonstrates the importance of the Canadian Charter for holding the government to its legislative mandate. The application of Section 8 to *foreign* surveillance, however, remains in question, particularly with respect to the access of foreign residents to remedies under the Canadian Charter.

To begin with, Section 8 applies to "[e]veryone," including "every human being who is physically present in Canada and by virtue of such presence amenable to Canadian law."[276] The extent of the Canadian Charter's application to foreign residents abroad, however, is contextual. As Justice L'Heureux-Dubé found in her dissenting opinion in *R. v. Cook*, "I am not convinced that passage of the Charter necessarily gave

---

[272] PIPEDA, *supra* note 39, § 7(3).

[273] Criminal Code, *supra* note 192, § 487.0195(1).

[274] R. v. Spencer, [2014] 2 S.C.R. 212 (Can.), https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do.

[275] *Id.*

[276] Singh v. Minister of Emp't & Immigration, [1985] 1 S.C.R. 177, ¶ 35 (Can.), https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/39/index.do.

rights to everyone in the world, of every nationality, wherever they may be, even if certain rights contain the word 'everyone.'"[277]

In *R. v. Hape*, the Supreme Court of Canada relied on Justice L'Heureux-Dubé's reasoning to hold that the Canadian Charter did not apply to an investigation of a Canadian businessman in the Turks and Caicos, carried out by the Turks and Caicos police force under local law but at the direction of the RCMP. The Court emphasized that the Canadian Charter's application is coextensive with the authority of the Canadian government:

> A criminal investigation in the territory of another state cannot be a matter within the authority of Parliament or the provincial legislatures, because they have no jurisdiction to authorize enforcement abroad. Criminal investigations, like political structures or judicial systems, are intrinsically linked to the organs of the state, and to its territorial integrity and internal affairs. Such matters are clearly within the authority of Parliament and the provincial legislatures when they are in Canadian territory; it is just as clear that they lie outside the authority of those bodies when they are outside Canadian territory.[278]

Subsequently, in *Canada (Justice) v. Khadr*, the Supreme Court held that the Canadian Charter did apply to the interrogation of a *Canadian citizen* by CSIS officials at Guantanamo Bay.[279] Unlike in *Hape*, the Court found that the interrogation violated Canada's human rights obligations, thereby eviscerating "the *Hape* comity concerns that would ordinarily justify deference to foreign law."[280] Since Canadian officials participated directly in the interrogation process, the Canadian Charter applied to their conduct.[281]

The Supreme Court of Canada has not confronted the question of the Canadian Charter's application to non-citizens abroad, but the issue was raised before the Federal Court in *Slahi v. Canada (Minister of Justice)*.[282] On facts almost identical to Khadr, also involving an interrogation at Guantanamo Bay, the Federal Court decided *not* to apply

---

[277] R. v. Cook, [1998] 2 S.C.R. 597, ¶ 86 (Can.), https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1653/index.do.

[278] R. v. Hape, [2007] 2 S.C.R. 292, ¶ 94 (Can.), https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2364/index.do.

[279] Canada (Justice) v. Khadr, [2008] 2 S.C.R. 125, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/4638/index.do.

[280] *Id.* ¶ 26.

[281] *Id.*

[282] Slahi v. Justice, [2009] F.C. 160 (Can.).

the Canadian Charter based on the critical distinction that the applicant was not a Canadian citizen. In order for the Canadian Charter to apply, the court held, there must be a sufficient "nexus to Canada," including "presence in Canada, a criminal trial in Canada, or Canadian citizenship."[283] For foreign citizens outside of Canada, the Canadian Charter applies "only in exceptional circumstances."[284]

While no Canadian court has confronted the question of the Canadian Charter's application to foreign surveillance, Canadian jurisprudence emphasizes that the application of the Canadian Charter depends on the extent to which Canadian authority was exercised in the situation in question. This formulation, however, leaves little clarity where Canadian authorities can target foreign actors, on Canadian and foreign networks, at the click of a mouse, without ever leaving their offices.[285]

At one extreme, if an EU resident was searched while traveling in Canada, Canadian Charter protections clearly would apply. Conversely, where Canadian officials intercept foreign communications abroad with the help of another country's security services, the nexus to Canada likely would be too attenuated. But, in between these extremes, the Canadian Charter's application is unresolved. For example, what happens if the Canadian government acquires personal data from a Canadian service provider that an EU resident had intentionally transferred to Canada for safekeeping? As one commentator noted, "there remains uncertainty as to whether Canadian authorities require some form of lawful authority to conduct surveillance abroad . . . even if the Charter does not apply."[286] As a result, the rights of foreign persons

---

[283] *Id.* ¶¶ 47–48.

[284] *Id.* ¶ 47.

[285] *See c.f. Microsoft Corp. v. U.S.*, 829 F.3d 197 (2d. Cir. 2016). At issue in the case was whether the U.S. could obtain from Microsoft, with a warrant, data that was stored on a server in Ireland. The outcome turned on the proper interpretation of the U.S. Stored Communications Act, which required consideration of the extent of U.S. authority to foreign data accessible online. At the trial court level, Judge Francis IV ruled that "the concerns that animate the presumption against extraterritoriality are simply not present here: an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. At least in this instance, it places obligations only on the service provider to act within the United States." *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 475-76 (S.D.N.Y. 2014).

[286] Lisa M. Austin, *Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State*, *in* LAW, PRIVACY AND SURVEILLANCE IN CANADA IN THE POST-SNOWDEN ERA 103-119 (Michael Geist & Wesley Wark eds., 2015).

abroad against Canadian searches may vary according to the method of search in ways unforeseeable to EU residents and unresolved in Canadian law.

2. Government Interception of Non-Private Communications Is Not Subject to Clear, Precise and Accessible Rules

The government's authority to intercept communications turns on whether the communications in question are considered "private." While, as discussed above, the Criminal Code prohibits public authorities from intercepting private communications, except under specific conditions, the interception of non-private communications largely falls outside the scope the legislative framework.

The Criminal Code defines "private communications" to include any telecommunications *from a person* in Canada, or *to a person* in Canada, where the originator has a reasonable expectation of privacy in the communication.[287] This leaves two significant gaps in protections for EU residents. First, to the extent that a communication involves only persons outside of Canada (and not Canadian citizens), the security agencies have much greater leeway to intercept it. To be sure, Canadian authorities are required, in all circumstances, to act consistently with their respective mandates.[288] Aside from abiding by these general mandates, however, no publicly accessible, precise rules govern the interception of purely foreign communications. As Craig Forcese

---

[287] *See* Criminal Code, *supra* note 192, at s. 183 ("*Private communication* means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.").

[288] For CSIS, this means they may collect information only to investigate "threats to the security of Canada" or "in relation to the defence of Canada or the conduct of international affairs." CSIS Act, *supra* note 216, §§ 12(1), 16(1). CSE may collect information only for the purposes of "foreign intelligence," which is defined as "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security." National Defence Act, *supra* note 243, § 273.61. The RCMP's mandate to investigate terrorism-related offenses arises under a number of acts, including the Security Offences Act, the Security of Information Act, the Anti-Terrorism Act, as well as the Criminal Code of Canada. ROYAL CANADIAN MOUNTED POLICE, *supra* note 189, ¶ 1.

concluded, "Put bluntly, for foreign spying there are no real legislated rules."[289]

Second, because of the opacity of national security programs, secret government interpretations could ostensibly set legal limits in classified internal interpretations, without the opportunity for any definitive judicial interpretation.[290] One former CSE Commissioner recognized, "there are ambiguities in the legislation as now drafted . . . . Currently, two eminent lawyers, the Deputy Minister of Justice and my independent Legal Counsel disagree over the meaning of key provisions that influence the nature of the assurance that I can provide."[291] Since these interpretations remain secret, legal protections may depend on an agency's shifting interpretations of the legislative mandate and ministerial authorizations, not on any concrete legal limits.[292]

This situation is exacerbated by the fact that the ministerial directives and authorizations that are being interpreted often remain secret themselves. Even when they emerge through Access to Information requests, they may be heavily redacted to the point of undermining all comprehension. In one recent example, a directive to the CSE on metadata collection, which was released to *The Globe and Mail*, was scrubbed of more than half of its text, including even the definition of metadata.[293]

In *Weber and Saravia v. Germany*, the ECtHR found that, at minimum, a statute must have safeguards in place "to avoid abuses of power," including by specifying "the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which

---

[289] Craig Forcese, *Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives*, *in* LAW, PRIVACY, AND SURVEILLANCE IN THE POST-SNOWDEN ERA 127, 130 (Michael Geist & Wesley Wark, eds., 2015).

[290] Austin, *supra* note 286, at 107–08.

[291] ANNUAL REPORT 2005–2006, COMMC'NS SEC. ESTABLISHMENT COMM'R (Apr. 2006), https://www.ocsec-bccst.gc.ca/a78/ann-rpt-2005-2006_e.pdf.

[292] Austin, *supra* note 286, at 107–08.

[293] *The 'Top Secret' Surveillance Directives*, THE GLOBE AND MAIL (Jun. 6, 2016, 11:32 AM), http://www.theglobeandmail.com/news/national/top-secret-surveillance-directives/article30249860/.

recordings may or must be erased or the tapes destroyed."[294] Canadian laws do not provide these minimum safeguards for communications that are not considered private, including by reason of the foreignness of the communicating parties. Moreover, because the government's legal interpretations often remain shrouded in secrecy, there is little clarity over which communications are private and which are not. Critics may therefore argue that Canadian law does not satisfy the clear rules prong.

3. Canada's Framework May Be Circumvented by Cooperation with the "Five Eyes" and Boomerang Routing

Snowden's leaks revealed unprecedented details about the degree of coordination and cooperation among the intelligence services of the "Five Eyes" nations – the U.S., UK, Australia, New Zealand, and Canada.[295] Information sharing also may extend beyond the Five Eyes. One report from the Snowden leaks, for example, indicated that the United States shared raw intelligence with Israel without placing any legal limits on Israel's use of the data.[296] Information sharing raises the concern that each country's spy agencies may engage in legal arbitrage: outsourcing spy operations to other countries to avoid legal restrictions on domestic spying. Such coordination undermines the foreseeability not only of the rules that apply to intelligence gathering by Canadian authorities, but also of the extent to which information in Canada may be accessed by Canada's partners.

Little is known about the information sharing policies among the Five Eyes, but the most detailed portrait is provided by a 2013 case from the Federal Court of Canada.[297] The case arose after the CSE Commissioner recommended, in his annual report, that the CSE should provide more information to the Federal Court of Canada "about the

---

[294] Weber & Saravia v. Germany, App. No. 54934/00, ¶ 95, (2006), http://hudoc.echr.coe.int/eng?i=001-76586.

[295] Nick Hopkins, *UK Gathering Secret Intelligence via Covert NSA Operation*, THE GUARDIAN (Jun. 7, 2013, 9:27 AM), https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism.

[296] Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, THE GUARDIAN (Sept. 11, 2013), https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[297] *In re* an application by [Redacted] for a warrant pursuant to Sections 12 and 21 of the Canadian Security Intelligence Service Act, R.S.C. 1985, c C-23; *In re* [Redacted], [2013] F.C. 1275, https://leaksource.files.wordpress.com/2013/12/mosley-csis.pdf [hereinafter *In re* X].

nature and extent of the assistance CSE may provide to CSIS."[298] Having issued warrants to CSIS to conduct surveillance on two individuals in 2009, Justice Mosley of Federal Court ordered CSIS and CSE to disclose whether CSE had provided assistance on the warrants he issued, and, if so, whether CSIS was required to disclose the assistance in its warrant application. It turned out that CSIS had, in fact, requested CSE's assistance and, moreover, CSE sought the assistance of foreign security services to collect intelligence abroad.[299]

The decision revealed the legal interpretations that undergird information sharing among foreign intelligence services. CSIS argued that it was not required to obtain a warrant to engage CSE's assistance, relying on an earlier decision holding that the Federal Court did not have the jurisdiction to authorize foreign interceptions that take place abroad on foreign equipment.[300] Additionally, the Deputy Attorney General of Canada asserted that because Canadian law did not apply extraterritorially, CSE could request assistance from foreign allies provided that the surveillance did not violate the foreign state's laws.[301] Thus, under this argument only the foreign state's laws applied to interceptions that occurred outside of Canada.

Justice Mosley rejected the government's approach, finding that CSIS was not permitted to engage CSE to do something that CSIS could not itself do.[302] At the time of the decision, Section 12 of the CSIS Act did not expressly state that it could pursue its activities "within or outside Canada." Thus, Justice Mosley relied on the presumption against the extraterritorial application of law, concluding that CSIS did not have the authority to engage foreign assistance through CSE without a warrant.[303]

Justice Mosley's decision revealed some of the machinery behind international intelligence-sharing. Now that the CSIS Act

---

[298] Craig Forcese, *Triple Vision Accountability and the Outsourcing of CSIS Intercepts*, NATIONAL SECURITY LAW: CANADIAN PRACTICE IN INTERNATIONAL PERSPECTIVE (Dec. 6, 2013, 8:35 AM), http://craigforcese.squarespace.com/national-security-law-blog/2013/12/6/triple-vision-accountability-and-the-outsourcing-of-csis-int.html.

[299] Colin Freeze, *CSIS Not Being Forthcoming With Court, Federal Judge Says*, THE GLOBE AND MAIL (Nov. 25, 2013, 10:42 PM), http://www.theglobeandmail.com/news/national/csis-not-being-forthcoming-with-court-federal-judge-says/article15599674/.

[300] *In re X*, [2013] 23 F.C. 1275, ¶ 33.

[301] *Id*. ¶ 34.

[302] *See* National Defence Act, *supra* note 243, § 273.64(3) ("Activities carried out under paragraph (1)(c) [CSE's assistance mandate] are subject to any limitations imposed by law on federal law enforcement and security agencies in the performance of their duties.").

[303] *In re* X, [2013] 23 F.C. 1275, ¶ 111.

expressly permits CSIS to act outside of Canada, it is not clear how a similar decision would turn out. Whenever CSIS or CSE authorizes an ally to conduct surveillance, "it takes the risk that another agency will act independently on the information," under the rules of its own sovereign.[304] From the perspective of EU residents, there are no clear and precise rules when Canadian-directed surveillance could be governed by the laws of any one of the FiveEyes countries and vice versa.

This lack of clarity is exacerbated by the way information flows across a borderless internet. Even where information is not intentionally shared with foreign allies, so-called "boomerang routing" could lead information transferred to Canada to be routed unintentionally outside of the country.[305] This is because Canadian internet providers frequently use US exchange points, even when routing wholly domestic traffic.[306] By one estimate, up to 90 percent of communications among Canadians may pass through the U.S.[307] Thus, once information is transferred to Canada pursuant to the adequacy decision, it may be scooped up by United States or other foreign surveillance.

Canada's participation in the Five Eyes partnership garnered scrutiny from European lawmakers in 2013. Following the Snowden disclosures, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs issued a report on US surveillance in which it noted Canada's active cooperation with the United States and its involvement "on a large scale in mass surveillance of electronic communications."[308] The report called on the European Commission to

---

[304] Tamir Israel, *Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation*, *in* LAW, PRIVACY, AND SURVEILLANCE IN THE POST-SNOWDEN ERA 71, 89 (Michael Geist & Wesley Wark eds., 2015).

[305] *See* Andrew Clement & Jonathan A. Obar, Canadian Internet "Boomerang" Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges, in LAW PRIVACY AND SURVEILLANCE IN CANADA IN THE POST-SNOWDEN ERA 13 (Michael Geist & Wesley Wark eds., 2015) (detailing how communications within Canada may be routed through the United States).

[306] *Id.*

[307] Mitch Potter & Michele Shephard, *Canadians Not Safe From U.S. Online Surveillance, Expert Says*, THE TORONTO STAR (Jun. 7, 2013), https://www.thestar.com/news/world/2013/06/07/canadians_not_safe_from_us_online_surveillance_expert_says.html.

[308] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs of the Committee on Civil Liberties, Justice and Home Affairs, (Jan. 8, 2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-

assess "whether the adequate level of protection of . . . the Canadian Personal Information Protection and Electronic Documents Act [has] been affected by the involvement of their national intelligence agencies in the mass surveillance of EU citizens."[309] As this section demonstrates, should the Commission take up this mandate, it might be troubled by the opacity of Canada's framework for sharing intelligence with its partners.

F. STRICTLY NECESSARY AND PROPORTIONATE

The second prong of the *Schrems* test asks whether the legal framework limits surveillance to only what is strictly necessary and proportionate to a national security interest. Article 52(1) of the EU Charter states, "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms." Derogations from EU Charter rights must meet "the principle of proportionality" and will be found valid "only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[310]

In *Digital Rights Ireland*, the CJEU laid out a four-part test for applying the requirements of Article 52(1). First, the Court asked whether the law at issue "adversely affect[ed] the essence" of an EU Charter right.[311] A law that violates the essence of a right is presumptively invalid.[312] Second, the Court considered whether the law genuinely served "an objective of general interest."[313] A law directed at national security and combatting terrorism satisfies this criterion.[314] Third, the law must be proportionate to the objective and, finally, it must be "strictly necessary" to achieve its goal.[315]

%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0%2F%2FEN.

[309] *Id.*

[310] EU Charter, *supra* note 22, art. 52(1).

[311] Digital Rights Ireland, *supra* note 26, ¶¶ 39-40.

[312] Case C-300/11, ZZ v. Sec'y of State for the Home Office, 2013 E.C.R. 363, ¶¶ 51, 54. *See also* Kuner, *supra* note 154, at 21 ("Thus, under the Charter, such access [violating the essence of a fundamental right] is per se unlawful, without the need for a balancing test.").

[313] Digital Rights Ireland, *supra* note 26, ¶¶ 41–44.

[314] *Id.* ¶ 42.

[315] *Id.* ¶¶ 44–52.

1. Interception of Foreign-to-Foreign Communications Abroad

The definition of "private communications" under Canadian law is expansive. It includes "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada."[316] Obviously excluded from this definition, however, are communications between two foreign residents outside of the country, for example, between a French citizen and a German citizen in Belgium. As is clear from the discussion above, only private communications – that is, where one of the communicating parties is Canadian or physically present in Canada – acquire meaningful protections under Canadian law.

This section addresses foreign-to-foreign communications. Communications between an EU resident and a person in Canada are addressed in the next section.[317] Communications between foreign residents that are not "intercepted" but rather are accessed as stored records in Canada are discussed in a separate section on the government's right to access stored records.[318]

Canada's legal framework for intercepting foreign-to-foreign communications may fall short of the aspirations of the EU Charter. Since these communications are not considered private, they largely remain outside of Canada's legal framework and their interception is subject to few constraints. However, such practices, if they exist, should have little relevance for an adequacy determination, since they do not impact data transferred under Europe's data protection regime. An adequacy review should not focus on Canada's surveillance apparatus writ large, but rather only on surveillance activities insofar as they potentially affect data transferred from the EU to Canada under the Data Protection Directive.

Article 25 of the Data Protection Directive compels consideration of "the rules of law, both general and sectoral, in force in the third country."[319] Paragraph 2 makes clear that these rules must be assessed "in the light of all the circumstances *surrounding a data transfer operation or set of data transfer operations*" (emphasis

---

[316] Criminal Code, *supra* note 192, § 183.

[317] *See infra* Part IV.B.ii.

[318] *See infra* Part IV.B.iv.

[319] Data Protection Directive, *supra* note 1, at art. 25(1) (EC).

added).[320] Foreign communications that are intercepted in Europe or elsewhere outside of Canada are not transferred to Canada pursuant to the adequacy decision. Instead, if this type of interception occurs and if the intercepted data is subsequently transferred by Canadian authorities back to Canada for analysis, such a transfer would not be subject to the adequacy decision since Canadian authorities are subject to neither the Data Protection Directive nor PIPEDA.[321]

Despite the distinction Canadian law makes between foreign-to-foreign and foreign-to-Canadian communication, Europeans may be as troubled by the interception of European communications outside of Canada as they would be by interception within Canada. However, the practice of the European Commission confirms that adequacy review assesses only the protection afforded to information transferred from Europe pursuant to an adequacy decision (or some other data transfer mechanism). For example, when Israel applied for an adequacy decision in 2010, Ireland voiced a last minute objection to the approval of the application because Israel allegedly had used forged Irish passports in the reported killing of a Hamas militant in Dubai.[322] Irish government officials expressed concern about the data practices of Israeli security agencies, such as Mossad, and their potential impact on Europeans' data. Despite Ireland's objection, Israel ultimately obtained adequacy, ostensibly demonstrating that the scope of the European Commission's review was limited to assessing strictly data transfers that fall under the adequacy decision.[323]

In the case of the EU-US Safe Harbor Framework, adequacy was limited to companies that voluntarily self-certified to a set of agreed upon principles. This narrow approach to adequacy analysis was sanctioned by the CJEU, which found that "a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of

---

[320] *Id.* at art. 25(2).

[321] Canadian Adequacy Decision, *supra* note 53, at art. 1 (EC) (authorizing the transfer of personal data "to recipients subject to the Personal Information Protection and Electronic Documents Act"); *see also* PIPEDA, *supra* note 39, § 4(1) (PIPEDA's scope is limited to "organization[s that] collect[], use[] or disclose[personal information] in the course of commercial activities," thereby excluding the public sector from its reach).

[322] Laurence Peter, *Ireland Delays EU Deal with Israel on Data Transfers*, BBC NEWS (Sept. 3, 2010), http://www.bbc.com/news/world-europe-11176926.

[323] Commission Decision 2011/61/EU of 31 January 2011 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by the State of Israel with Regard to Automated Processing of Personal Data, 2011 O.J. (L 27) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415701992276&uri=CELEX:32011D0061.

Directive 95/46."[324] Instead of addressing US surveillance laws writ large, including *vis-à-vis* US citizens or the citizens of other countries, the Court's focus was squarely on securing assurances for "persons whose data has been transferred from the European Union to the United States" under the Safe Harbor Decision.[325]

This accords with Max Schrems's complaint to the Irish DPC, which asked the DPC to investigate whether data transferred by Facebook pursuant to Safe Harbor was improperly accessed in transit or in the United States under the alleged PRISM program.[326] Schrems did not raise any issues concerning US access to European data outside of Safe Harbor-certified companies or even to US access to data held by Safe Harbor-certified companies in Europe. Indeed, Schrems would not have been able to bring such a claim under the data transfer provisions of the Data Protection Directive, since in that scenario, there would not have even been a cross border data transfer.[327] Therefore, because the Data Protection Directive does not apply, the absence of Canadian protections for foreign-to-foreign interceptions is not fatal to Canada's adequacy.

2. Interception of European-Canadian Communications

Although in *Schrems* the CJEU did not assess US surveillance law head on, it concluded that the collection of "*all* the personal data of *all* the persons whose data has been transferred from the European Union to the United States" would violate the strict necessity requirement.[328] In *Digital Rights Ireland*, the CJEU found that the Data Retention Directive failed to meet the necessity requirement because the law's broad application meant that it would impact "persons for whom there is no evidence capable of suggesting that their conduct might have a link, even

---

[324] Schrems [2014] IEHC 310, ¶ 81.

[325] *Id.* ¶ 93.

[326] Schrems v. Data Protection Comm'r [2014] IEHC 310, Complaint against Facebook Ireland Ltd – 23 "PRISM," (Ir.), http://www.europe-v-facebook.org/prism/facebook.pdf.

[327] To be sure, if Facebook provided the NSA access to the data in Ireland, Schrems might have had a valid complaint under other provisions of the Data Protection Directive. But such a complaint would not trigger the data transfer provisions of the Data Protection Directive because access would have occurred on European soil, before any data transfer had taken place. Any subsequent transfer of that data from Ireland to the U.S. by the NSA, moreover, would have been outside the scope of the Data Protection Directive, which does not apply to European intelligence agencies, much less to the NSA.

[328] Schrems [2014] IEHC 310, ¶ 91 (emphasis added).

an indirect or remote one, with serious crime."[329] Whether the EU Charter permits more limited "bulk" surveillance—such as an agreement between the EU and Canada to share passenger name records ("PNR")[330] or Member State legislation that requires telecommunications service providers to retain metadata, but allows the government to access such data only under specific conditions[331]—is now before the CJEU for review.

To meet the EU standard, therefore, data transfers from the EU to Canada must be protected under Canadian law. As explained above, Canadian protections from interception apply only to "private communications."[332] Although these laws were designed with telephone wiretapping in mind, a communication under the Criminal Code may be "any oral communication, or any telecommunication,"[333] including "the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system."[334] This definition appears to be sufficiently broad so as to encompass the interception of any data in transit over the internet, regardless of whether it is a telephone conversation between two individuals or a transfer of data files from business to business.

---

[329] Digital Rights Ireland, *supra* note 26, ¶¶ 56–58.

[330] *See Opinion A-1/15, EU-Canada PNR Agreement*, EUROPEAN CRIMINAL LAW ACAD. NETWORK (2016), http://eclan.eu/en/eu-case-law/opinion-1-15-eu-canada-pnr-agreement. *See also Opinion of the Advocate General Mengozzi, Opinion 1/15* 2016, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=726777 (recommending the Court to strike down the Canada-EU PNR agreement because it allows for the Canadian government to access and share European data for reasons not connected to serious crimes).

[331] *See generally* CJEU, Joined Cases C-203/15 and C-698/15. On July 19, 2016, the CJEU Advocate General issued a non-binding opinion on the joined cases, finding that Member State legislation requiring telecommunications service providers to retain metadata does not necessarily violate the EU Charter, as long as the legislation restricts government access to the data only to what is strictly necessary and proportionate for combating "serious crimes." Court of Justice of the European Union Press Release 79/16, Advocate General's Opinion in Joined Cases C-203/15 Tele2 Sverige AB v. Post-och telestyrelsen and C-698 Secretary of State for Home Department v. Tom Watson and Others, (July 19, 2016). *See also* Data Protection Working Party, *supra* note 162, at 39 ("So far, there is no conclusive jurisprudence on the legality of massive and indiscriminate data collection and subsequent use of personal data for the purpose of combating crime, including the question under what circumstances such collection and use of personal data could take place.").

[332] Criminal Code, *supra* note 192, § 184(1).

[333] *Id.* § 183.

[334] Interpretation Act, R.S.C. 1985, c. I-21, s. 35.

To qualify as a "private communication" under Canadian law, a data transfer from Europe must involve a communication "intended by the originator to be received by a person who is in Canada,"[335] along with a "reasonable expectation of privacy." In *R. v. Law*, the Canadian Supreme Court recognized a "liberal approach to the protection of privacy" that "extends not only to our homes and intimately personal items, but also to information which we choose . . . to keep confidential."[336] This right to "informational privacy," the Court subsequently held, includes "'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'"[337] In *Law*, relying on the right to informational privacy, the Court held that a restaurant owner had a reasonable expectation of privacy in "confidential business documents" – including a checkbook and a ledger of disbursements – that were discovered in a stolen safe.[338]

Under the logic of *Law*, business records transferred to Canada pursuant to the adequacy decision likely qualify as private communications when the facts demonstrate an intent to keep the records confidential. To the extent that an expectation of privacy in these transfers is reasonable, any interception by the Canadian government must be subject to the legal limits outlined above.[339]

In order to obtain an intercept warrant, the RCMP must specify the facts relied on to support a reasonable belief that an offense is likely to be committed, the names and addresses of the targets of the investigation (if known), the type of private communication that will be intercepted, and a general description of the manner in which it will be intercepted.[340] While, in addition to these requirements, the RCMP usually needs to demonstrate investigative necessity to obtain such a warrant, it is not required to do so for terrorism and criminal organization-related offenses.[341] Instead, for such investigations, the RCMP must meet only the "reasonable grounds to believe" standard.

---

[335] Criminal Code, *supra* note 192, § 183.

[336] R. v. Law, [2002] 1 S.C.R. 227, ¶ 16. (Can.).

[337] R. v. Tessling, [2004] 3 S.C.R. 432, ¶ 23 (Can.) (quoting Alan F. Westin, PRIVACY AND FREEDOM 7 (1970)).

[338] R. v. Law, [2002] 1 S.C.R. 227, ¶ 16. (Can.).

[339] *See supra* Part III.

[340] Criminal Code, *supra* note 192, § 185(1).

[341] *Id.* § 185(1.1).

This framework prevents the collection of *all* data transferred from the EU to Canada, since the RCMP may intercept communications only when there is a reasonable belief that an offense was committed. However, depending on the CJEU's resolution of the PNR case, it may, nonetheless, fall short of the strict necessity requirement. Te framework may even fall short of the Canadian constitutional protections.[342] In *R. v. Araujo*, the Canadian Supreme Court stated, in dicta, that "the investigative necessity requirement embodied in s. 186(1) is one of the safeguards that made it possible for this Court to uphold these parts of the Criminal Code on constitutional grounds."[343] Given its shaky constitutional status in Canada, the lack of an investigative necessity requirement in the case of terrorism-related offences may be viewed by the CJEU as authorization for disproportionate interception, posing a challenge to Canadian adequacy under EU law.

Interestingly, CSIS's wiretapping framework is more likely to pass muster under CJEU review. The CSIS framework "protects privacy at least as robustly as part VI of the [Criminal] Code," which regulates RCMP interceptions.[344] CSIS warrants are issued under similar conditions to those that apply to the RCMP,[345] except that CSIS is bound by an additional obligation to collect information only "to the extent that it is strictly necessary" under its Section 12 mandate.[346] While CSIS does not face such a restriction when acting under its Section 16 mandate to provide assistance to the Ministers of Defense and Foreign Affairs, it must, regardless of the mandate, demonstrate investigative necessity – that other measures have been tried and failed or the matter is too urgent to use other measures – in order to intercept private communications.[347] Thus, for communications between EU residents and Canadians, the CSIS Act likely limits interception to what is strictly necessary and proportionate.

Of the national security agencies, CSE has the broadest mandate for collecting foreign intelligence.[348] It may, with a ministerial

---

[342] Penney, *supra* note 198, at 260.

[343] R. v. Araujo, [2000] 2 S.C.R. 992, ¶ 26 (Can.).

[344] Penney, *supra* note 198, at 270.

[345] *See supra*, Part IV.B.

[346] CSIS Act, *supra* note 216, § 12(1).

[347] *See id.* § 21(2)(b).

[348] Christopher Parsons, Telecom Transparency Project The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians 16-19 (2015), https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

authorization and no judicial warrant, intercept communications "in relation to an activity or class of activities specified in the authorization."[349] Such interception must be directed at foreign entities outside of Canada, justified by the expected value of the foreign intelligence, and the information must not be obtainable by other means.[350] Once collected, CSE must put in place measures to minimize the use or retention of private communications "to protect the privacy of Canadians."[351]

The European proportionality requirement, which implies a balance between individual interests and the state's interest, may be partially satisfied by CSE's duty to demonstrate that "the expected foreign intelligence value of the information that would be derived from it justifies it."[352] Furthermore, the framework embeds an element of investigative necessity by requiring CSE to demonstrate that "the information to be obtained could not reasonably be obtained by other means."[353]

A significant shortcoming of this framework, though, is that it does not require CSE to identify any specific individuals as targets of surveillance. Instead, CSE may secure a ministerial authorization to intercept communications related to "a class of activities."[354] Furthermore, the requirement to minimize privacy impacts is intended "to protect the privacy of Canadians,"[355] and, therefore, may not apply to EU residents at all. In the absence of meaningful oversight, CSE's interpretations of its own authority may be even broader than a straightforward reading of the statute.[356] According to one CSE Commissioner's report, "the Minister need only authorize 'classes of communications interception activities,' as opposed to interceptions of private communications in relation to specific activities or targets."[357] Thus, this framework might ostensibly allow CSE to filter *all* internet traffic arriving from outside of Canada.

---

[349] *See* National Defence Act, *supra* note 243, § 273.65(3).
[350] *Id.*
[351] *Id.* at 273.65(2)(d).
[352] *Id.* at 273.65(2)(c).
[353] *Id.* at 273.65(2)(b).
[354] *Id.* at 273.65(3).
[355] National Defence Act, *supra* note 243, at 273.65(2)(d).
[356] Austin, *supra* note 286, at 110–11.
[357] Israel, *supra* note 304, at 78–79.

CSE's framework does provide protection for the subsequent use and retention of collected data.[358] The Minister of National Defence must ensure that "private communications will be used or retained only if they are *essential* to international affairs, defence or security."[359] While a straightforward definition of "essential" includes the concept of necessity,[360] the fact that this requirement does not limit the initial collection may conflict with the EU Charter.[361] The inclusion of "international affairs" as a basis for data use and retention, moreover, without further elaboration, may extend beyond the objectives that justify an intrusion upon an EU Charter right.[362] While *Schrems* did not rule on the US surveillance apparatus, and the question of limited bulk collection now awaits CJEU review, this type of collect-then-minimize interception appears to be at the heart of the CJEU decision.

3. Interception of Communications Metadata

The Snowden disclosures thrusted the national security use of metadata into the international limelight.[363] Metadata is "data that

---

[358] *See generally* National Defence Act, *supra* note 243, at 273.65(2)(d).

[359] *Id.*

[360] The Oxford English Dictionary defines "essential" as "absolutely necessary; extremely important," or "fundamental or central to the nature of something or someone." *Essential*, OXFORD ENGLISH DICTIONARY, http://www.oed.com/view/Entry/64503?redirectedFrom=essential& (last visited Nov. 11, 2016). Although not explicitly defined under Canadian law, the Public Service Labour Relations Act equates "essential services" to services that are "necessary for the safety or security of the public." Public Service Labour Relations Act, S.C. 2003, c 22, § 119(1) (Can.).

[361] *See* Data Protection Working Party, *supra* note 162, at 40 (stressing that, although the legality of "targeted, but massive data processing" remains unsettled, if allowed, "the targeting principles should apply to both the collection and the subsequent use of the data, and cannot be limited to just the use").

[362] *See* Digital Rights Ireland, *supra* note 26, ¶ 60 (striking down the Data Retention Directive in part because it left the definition of "serious crime" to Member State law, without providing additional guidance). In October, 2013, documents released by Snowden revealed that CSE may have targeted Brazil's Mines and Energy Ministry. Although the rationale for the alleged spying is not known, a former CSIS senior intelligence officer stated in an interview, "So where do we do [economic espionage] and against who are we doing it? Basically, everywhere and everybody that has involvement with our national security issue. The concept of economic security is part of national security as well." Mark Gollom, *Brazil-Canada Espionage: Which Countries are We Spying On?*, CBC NEWS, Oct. 9, 2013, http://www.cbc.ca/news/canada/brazil-canada-espionage-which-countries-are-we-spying-on-1.1930522. Europeans may be troubled that Canada's surveillance laws seemingly permit such broad-based economic espionage.

[363] In fact, the first story of the Snowden disclosures revealed an NSA program to collect the bulk telephony metadata of Verizon subscribers. Glenn Greenwald, *NSA Collecting Phone Records of Verizon Customers Daily*, THE GUARDIAN, Jun. 6, 2013,

provides information about other data" and is generated as a person uses technology.[364] This type of data may reveal "time and duration of a communication, the particular devices, addresses, or numbers contacted, which kinds of communications services we use, and at what geolocation."[365] Like the NSA's activities, Canada's interception of metadata, mostly conducted by the CSE, also has come under heavy scrutiny following revelations of the breadth of the CSE's program.[366]

The legal framework applying to the interception of telecommunications metadata is not entirely settled. First of all, the definition of "private communication" leaves uncertainty over the legal regime that applies to the interception of communications metadata.[367] To qualify as a private communication, metadata must meet the definition of "telecommunication,"[368] which includes "signs, signals, writing, images, sounds or intelligence of any nature."[369]

Unlike the third party doctrine in the United States, which excludes from Fourth Amendment protection information that a person voluntarily turns over to a third party, such as metadata,[370] Canadian law does not automatically bar such information from constitutional

---

https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Those revelations launched several lawsuits and led to the amendment of U.S. access laws. Ewen MacAskill, *The NSA's Bulk Metadata Collection Authority Just Expired. What Now?*, THE GUARDIAN, Nov. 28, 2015, https://www.theguardian.com/us-news/2015/nov/28/nsa-bulk-metadata-collection-expires-usa-freedom-act. Six months after the first revelations, Snowden revealed that "[t]he National Security Agency is storing the online metadata of millions of internet users for up to a year, regardless of whether or not they are persons of interest to the agency." James Ball, *NSA stores metadata of millions of web users for up to a year, secret files show*, THE GUARDIAN, Sept. 30, 2013, https://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

364 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, METADATA AND PRIVACY: A TECHNICAL AND LEGAL OVERVIEW 1 (2014); *see* Paula H. Kift & Helen F. Nissenbaum, *Metadata in Context – An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program*, 13 ISJLP (forthcoming 2017), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800159; *see also* Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391 (2014).

365 Ann Cavoukian, A Primer on Metadata: Separating Fact from Fiction 3 (2013).

366 Colin Freeze, *Data-Collection Program Got Green Light from MacKay in 2011*, GLOBE & MAIL, Jun. 10, 2013, http://www.theglobeandmail.com/news/politics/data-collection-program-got-green-light-from-mackay-in-2011/article12444909/.

367 *See supra* Part IV.A.ii.

368 *See* Criminal Code, *supra* note 192, § 183.

369 Interpretation Act, *supra* note 334.

370 *See* United States v. Miller, 425 U.S. 435, 442 (1976) (holding that the petitioner did not have a reasonable expectation of privacy in his bank records because they contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business").

protection. Rather, the Canadian Supreme Court held, "[w]here a police officer requests disclosure of information relating to a suspect from a third party, whether there is a search depends on whether, in light of the totality of the circumstances, the suspect has a reasonable expectation of privacy in that information."[371]

In *R. v. Telus Communications*, as the Supreme Court of Canada confronted the question of whether a text message was a private communication, a plurality of the Court concluded, in dicta, that the definition of telecommunication extends beyond the communication itself to include "informational content – the substance, meaning, or purport – of the private communication . . . [and] any derivative of that communication that would convey its substance or meaning."[372] Lower courts that have confronted the question directly, however, remain divided.[373] While the Supreme Court found, in one context, that a person may have a reasonable expectation of privacy in subscriber data, even if it is held by a third-party,[374] lower courts have found, in other contexts, that any expectation of privacy in such third-party-held metadata was not reasonable.[375]

There is reason to believe that metadata plays a central role in CSE's signals intelligence activities.[376] Leaked documents reveal that from 2005 to 2011, CSE took the position that metadata were not private communications, and, therefore, collection could take place without ministerial authorization.[377] But the agency's position may have since changed.[378] By 2014, the agency acknowledged the privacy implications

---

[371] R. v. Spencer, [2014] 2 S.C.R. 212, ¶ 67 (Can.).

[372] R. v. TELUS Commc'n., [2013] 2 S.C.R. 3, ¶ 25 (Can.).

[373] *See* Craig Forcese, *Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives*, *in* LAW, PRIVACY AND SURVEILLANCE IN CANADA IN THE POST-SNOWDEN ERA 127, 138-39 (Michael Geist ed., 2015) (finding that some courts adhere to the view that "private communication involves the exchange of information between originator and recipient, not the fact that a means of communication has been engaged," (citations omitted) while others have found that metadata qualifies as private communications).

[374] R. v. Spencer, [2014] 2 S.C.R. 212, ¶¶ 65-66 (Can.).

[375] *See* Forcese, *supra* note 373, at 138–39 ("Yet a third, more recent category of cases has agreed that data created by these devices are telecommunications under Part VI, but that the concept of private communication has no bearing where the communicator knows some or all of it will or might be collected by the phone company in the normal course of business." (citations omitted)).

[376] *Metadata and our Mandate*, COMM. SECURITY ESTABLISHMENT, https://www.cse-cst.gc.ca/en/inside-interieur/metadata-metadonnees (last modified Jan. 28, 2016). ("Without metadata, we would not be able to effectively direct our resources and capabilities to keep Canada and Canadians safe and secure.").

[377] Forcese, *supra* note 373, at 135.

[378] *Id.*

of metadata collection.[379] Nonetheless, CSE's public statements reveal that, even if metadata is collected pursuant to ministerial authorization, the agency does not need to apply the same minimization standards for metadata concerning foreigners that it does for Canadians.[380]

Indeed, all of CSE's secretive metadata activities may be governed by a single directive that is just three pages long.[381] A former chief of the CSE alleged that the agency "is gathering huge amounts of so-called metadata from phone companies and internet providers, information on large numbers of people including their complete phone and email records."[382] Moreover, according to CSE Commissioner Jean-Pierre Plouffe, "metadata is acquired without having gone through a targeting selection process" and since the program's inception "the volume of metadata collected has increased considerably."[383]

The CSE Commissioner's 2015 report, disclosed to Parliament in January 2016, revealed that CSE failed to protect even the privacy of Canadians when it shared metadata with international allies without applying appropriate minimization standards.[384] As a result, the Minister of Defence was forced to suspend metadata sharing with international partners.[385] In a letter to the Minister of Defence, the CSE Commissioner recommended "that the National Defence Act be amended in order to clarify CSE's authority to collect, use, retain, share and disclose metadata."[386]

In contrast to Canadian law, which has left the treatment of metadata unresolved, the CJEU has concluded that the acquisition of metadata, specifically, subscriber data, does implicate the fundamental

---

[379] Ian MacLeod, *Canadian Electronic Spy Agency's Unlawful Metadata Sharing went on for Years Before Being Fixed*, NATIONAL POST, Feb. 22, 2016, http://news.nationalpost.com/news/canada/canadian-politics/canadian-electronic-spy-agencys-unlawful-metadata-sharing-went-on-for-years-before-being-fixed.

[380] COMM. SECURITY ESTABLISHMENT, *supra* note 376.

[381] *The 'Top Secret' Surveillance Directives*, GLOBE & MAIL, Jun. 2, 2016, http://www.theglobeandmail.com/news/national/top-secret-surveillance-directives/article30249860/.

[382] Greg Weston, *Spy Agency CSEC Needs MPs' Oversight, Ex-Director Says*, CBC NEWS, Oct. 7, 2013, http://www.cbc.ca/news/politics/spy-agency-csec-needs-mps-oversight-ex-director-says-1.1928983.

[383] Colin Freeze, *Spy Agency Accidentally Shared Canadians' Data with Allies for Years*, GLOBE & MAIL, Jun. 1, 2016, http://www.theglobeandmail.com/news/national/spy-agency-accidentally-shared-canadians-data-with-allies-for-years/article30243491/.

[384] *Canada's Electronic Spy Agency Stops Sharing Some Metadata with Partners*, CBC NEWS Jan. 28, 2016, http://www.cbc.ca/news/politics/spy-canada-electronic-metadata-1.3423565.

[385] *Id.*

[386] Freeze, *supra* note 383.

right to privacy, and, therefore, derogations from this right must satisfy the requirements of necessity and proportionality.[387] Meanwhile, under Canadian law, "[w]ith a broad-based ministerial authorization on metadata collection seemingly establishing few limits, the metadata program now represents one of the most significant privacy-related concerns with Canadian surveillance practices."[388] Consequently, faced with review under the European standard, the CJEU may very well find, like the CSE Commissioner, that the framework governing metadata collection lacks articulable standards that assure necessity and proportionality.

4. Access to Stored Communications and Business Records

A key issue for Canada's adequacy determination will be the extent to which the government can access stored records for national security purposes.[389] Canada's laws provide a clear standard, allowing a public official to obtain judicial authorization to access stored records upon showing "reasonable grounds to believe" that the records will produce evidence of a crime that has been or will be committed.[390] This standard creates an effective limit where the authorization is directed at an *individual*, as it requires law enforcement to identify the person of interest as well as the documents in their possession that are relevant to the investigation. These limits break down, however, where an authorization is directed at a *service provider* that stores information related to many individuals.

The Criminal Code requires the government to specify the person whose documents will be searched (for example, an ISP), but not the individuals who will be implicated in those documents.[391] Thus, subject only to the limitations imposed by the Canadian Charter, these

---

[387] Digital Rights Ireland, *supra* note 26, ¶ 39.

[388] Michael Geist, *Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era*, *in* LAW, PRIVACY, AND SURVEILLANCE IN CANADA IN THE POST-SNOWDEN ERA 225, 233 (Michael Geist ed., 2015)

[389] In *Schrems*, although the CJEU did not directly evaluate U.S. national security laws, the judgment made reference to the alleged PRISM program, an NSA program for accessing stored records, as an illustration of unlimited access. Schrems [2014] IEHC 310, ¶ 22.

[390] Criminal Code, *supra* note 192, § 487.014.

[391] See generally id.; see also Curtis Fudge, On March 10, 2015, Bill C-13 Came Into Effect. The Bill is Known as the Protecting Canadians from Online Crime Act, APA NEWSLAW (Mar. 11, 2015, 11:41 AM), https://apanewslaw.wordpress.com/2015/03/11/on-march-9-2015-bill-c%E2%80%9013-came-into-effect-the-bill-is-known-as-the-protecting-canadians-from-online-crime-act/.

warrants potentially allow the government to obtain access to vast stores of data held by a service provider. The law also allows the government to request voluntary disclosure, potentially leaving privacy protection at the discretion of third-party service providers that hold the data.[392]

According to official statistics, in 2010, the RCMP requested customer name and address information from telecommunications service providers in Canada at least 28,143 times.[393] In 93.6 percent of those cases, the service providers handed over information voluntarily.[394] One service provider alone reported that it responded to more than 2,500 production orders in a single year.[395] There are no known statistics on the extent to which the government has requested the *content* of communications rather than just the corresponding metadata. The RCMP itself maintained no comprehensive database of all access requests.[396]

Courts have addressed the potential breadth of such orders in the context of challenges under Section 8 of the Canadian Charter. In *R. v. Spencer*, discussed above,[397] the Supreme Court ruled that the Canadian Charter prevented the RCMP from acquiring subscriber information about a Canadian individual from a telecommunications service provider without a warrant .[398] Subsequently, the Court ruled that the police could not use a general warrant to access future text messages stored by the service provider incidentally to their delivery. Even though the police sought access to information that would be stored by the service provider, the Court held that the police were required to obtain an intercept warrant to collect *prospective* communications.[399]

These narrowing rulings, however, limited the scope of general warrants, which are based on the "reasonable grounds to believe standard." In 2014, the Canadian government enacted Bill C-13, which introduced a lower standard, "reasonable grounds to suspect" or "reasonable suspicion," for warrants to access transmission and subscriber data.[400] The reasonable suspicion standard, in this context, has

---

[392] PARSONS, *supra* note 348, at 22.

[393] *Id.*

[394] *Id.*

[395] R. v. Rogers Comm. P'ship, 2016 ONSC 70, ¶ 9, http://bit.ly/29Tn8fc.

[396] *See generally* Michael Geist, *RCMP Records are Called 'Incomplete and Inaccurate' in Memo*, TORONTO STAR (Feb. 27, 2015), https://www.thestar.com/business/2015/02/27/rcmp-records-called-incomplete-and-inaccurate-in-memo-geist.html.

[397] *See supra* Part IV.A.i.

[398] R. v. Spencer, [2014] 2 S.C.R. 212 (Can.).

[399] *See generally* R. v. TELUS Comm'ns Co., [2013] 2 S.C.R. 3, 4 (Can.).

[400] Protecting Canadians from Online Crime Act, S.C. 2014, c 31, s. 487.016 (Can.).

not yet faced judicial review. However, a recent case from the Ontario Superior Court of Justice demonstrates the privacy risks at stake. In *R. v. Rogers Communications Partnership*, police obtained a warrant for the subscriber information of all cellular phones that connected to a particular cell tower on a particular date (known as a "tower dump") using a general production order.[401] Although the warrant had been issued under the more rigorous "reasonable grounds to believe" standard, two service providers complained that "99.9% of the records sought will relate to innocent persons."[402] The court sustained the challenge, holding that "the Production Orders authorized unreasonable searches."[403]

Seeing as the government had sought such broad authority under the reasonable grounds standard, the new, lower standard may embolden the government to request ever-greater access to stored records. A recent report, for example, revealed that, as part of an investigation of a criminal organization, the RCMP obtained an encryption key that could unlock the communications of millions of BlackBerry mobile phones while they passed over the network.[404] While the FBI's attempt to secure a "backdoor" to bypass an iPhone's security measures resulted in a high-profile standoff in the United States,[405] the RCMP have allegedly had backdoor access to BlackBerry devices since 2010.[406]

Notwithstanding these shortcomings in the Canadian framework, Europeans might be reassured by the fact that, officially, access to stored documents by Canada's spy agencies is more circumscribed. CSIS must satisfy the same requirements to obtain a warrant to access stored communications as it does to intercept them, including demonstrating investigative necessity.[407] CSE's mandate is limited to collecting signals intelligence through "interception."[408] As of yet, no report has alleged that CSE had a program like the NSA's PRISM program to systematically access stored records in Canada.

---

[401] R. v. Rogers Comm. P'ship, 2016 ONSC 70, ¶ 9, http://bit.ly/29Tn8fc.

[402] *Id.* ¶ 25.

[403] *Id.* ¶ 43.

[404] Justin Ling & Jordan Pearson, *Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key*, VICE NEWS (Apr. 14, 2016, 8:00 AM), https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how.

[405] Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

[406] Ling & Pearson, *supra* note 404.

[407] CSIS Act, *supra* note 216, § 21(3).

[408] National Defence Act, *supra* note 243, at § 273.65(2).

5. Data Retention and Information Sharing

Canadian laws for data retention and information sharing raise additional adequacy concerns. In *Digital Rights Ireland*, the CJEU held that data retention laws must "contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use" and "the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary."[409] Although the RCMP and CSIS publicize their policies for retaining data, those policies are not enshrined in law and CSE does not publish its policies at all. In 2008, the Office of the Privacy Commissioner audited the RCMP's national security databank – which is exempt from the requirements of the Privacy Act – and found that the RCMP lacked a well-defined accountability infrastructure to ensure that its retention policies were actually implemented.[410] In fact, the report found that more than half of the files in the database should not have qualified for exempt databank status.[411]

These concerns have been exacerbated by Bill C-51 and the Security of Canada Information Sharing Act (SCISA) contained within it.[412] By allowing information sharing among federal agencies if information is "relevant" to "activities that undermine the security of Canada,"[413] SCISA allows information sharing "for an incredibly wide range of purposes, most of which have nothing to do with terrorism."[414]

In a submission to Parliament, the Privacy Commissioner expressed his concern that the relevance standard is "a much broader standard than that established elsewhere with respect to the collection of personal information."[415] Bill C-51, moreover, contained "no clear obligation for receiving institutions to discard information which does not meet their statutory collection standards, or to dispose of information

---

[409] Digital Rights Ireland, *supra* note 26, ¶¶ 62, 64.

[410] Privacy Comm'r of Can., Audit Report of the Privacy Commissioner of Canada Examination of RCMP Exempt Data Banks, A Special Report to Parliament (2008), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2008/nr-c_b-di_080213/.

[411] *Id.*

[412] SCISA, *supra* note 260, § 2.

[413] *Id.* § 5(1).

[414] Geist, *supra* note 388, at 236.

[415] Letter from Daniel Therrien, Commissioner, to Daryl Kramp, Chair, Standing Committee on Public Safety and National Security (Mar. 5, 2015), https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150305/.

once it has served its purpose."[416] This is especially troublesome because Bill C-51 allows information sharing when relevant to "activities that undermine the security of Canada," a class of activities that is likely broader than these covered by CSIS or the RCMP's mandates to protect against "threats to the security of Canada."[417] The end result is that shared information that exceeds an agency's mandate could wind up in legal limbo, where an agency may have no authority to use it, but also no requirement to delete it. The Privacy Commissioner warned that this gives the national security agencies "the potential to know everything about everyone" and the authority to "keep this information forever."[418]

G. INDEPENDENT OVERSIGHT

Under EU law, in addition to having clear and precise rules that limit access to what is strictly necessary and proportionate to a legitimate interest, national security legislation must include independent oversight to prevent the risk of abuse.[419] In *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, the ECtHR expressed its view regarding independent oversight, finding that oversight may vary in form as long as it continues to provide protection against abuse in practice.[420] While it was "in principle desirable to entrust supervisory control to a judge," the Court noted that it had previously approved measures that included review by "an independent body chaired by a president who was qualified to hold judicial office and which moreover had the power to order the immediate termination of the measures in question."[421] Thus, appropriate oversight may include a combination of judges, members of

---

[416] *Id.*

[417] KENT ROACH & CRAIG FORCESE, BILL C-51 BACKGROUNDER #3: SHARING INFORMATION AND LOST LESSONS FROM MAHER ARAR EXPERIENCE, 12 (Feb. 16, 2015), https://poseidon01.ssrn.com/delivery.php?ID=456095106112067002002097005023116074006004004021063037072112082105017096067105067085036126038056110028118080126123126021065119050082005021006118066071105091026018113067017085113083001097064116090072024026096023027068087126012095124025101102094019113127&EXT=pdf.

[418] Therrien, *supra* note 415 ("More problematic is the definition of "activities that undermine the security of Canada" which goes further than the existing definitions, untouched by SCISA, of "terrorist activity" in s. 83.01 of the Criminal Code and "threat to the security of Canada" in s.2 of the Canadian Security Intelligence Service Act (the CSIS Act).").

[419] Digital Rights Ireland, *supra* note 26, ¶ 62.

[420] Telegraaf Media Nederland Landelijke Media B.V. v. Netherlands (Judgment), App. No. 39315/06, Eur. Ct. H.R. ¶ 98 (2012), http://hudoc.echr.coe.int/eng?i=001-114439#{"itemid":["001-114439"]}.

[421] *Id.*; *see also* Klass and Others v. Germany (Judgment), 28 Eur. Ct. H.R. (ser. A) (1978).

the executive, parliamentary committees, or any other independent body.[422] The more a method of surveillance is prone to abuse, however, the more oversight will be required both in the form of prior approval and in the form of *ex post* review.[423]

Canada's national security oversight mechanisms suffer from two main shortcomings, particularly with regard to oversight of CSE.[424] The first issue is that CSE may conduct surveillance without any judicial oversight. In the absence of judicial oversight, especially over an agency that gathers large volumes of intelligence, European law mandates additional safeguards to protect against abuse. These safeguards should include some form of independent oversight as well as stringent review of the agency's activities.[425]

Under the National Defence Act, CSE must obtain authorization only from the Minister of National Defence, who is a political figure appointed to the cabinet by the Prime Minister.[426] The requirement that a minister tasked with establishing CSE's foreign intelligence priorities should also act "judicially when determining whether a particular privacy invasive activity is or is not justified" is "deeply problematic."[427]

The second issue is that there are significant weaknesses in Canada's *ex post* review of intelligence gathering.[428] A study by the European Parliament concluded that Canada stands out as a Western democracy that does not have active Parliamentary oversight over

---

[422] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *supra* note 152, at 29.

[423] Jacques Bourgeois et al., Sidley Austin LLP, Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States 22-23 (Jan. 25, 2016), http://www.sidley.com/~/media/publications/essentially-equivalent—-final.pdf [hereinafter Essentially Equivalent].

[424] For a detailed view of Canadian oversight, see Craig Forcese & Kent Roach, BILL C-51 BACKGROUNDER #5*:* OVERSIGHT AND REVIEW: TURNING ACCOUNTABILITY GAPS INTO CANYONS? (Feb. 26, 2015), https://poseidon01.ssrn.com/delivery.php?ID=909090025124094082073071090069125086002052029048028062025125102077113124065000002024100038101125051104060003086099007123065108016019030019052025101098092031100084011072053021068108068122001089003115019067109002106064026127008118087121077024066067073002&EXT=pdf.

[425] *See* Kennedy v. United Kingdom, App. No. 26839/05 Eur. Ct. H.R. (2010) (upholding the UK's oversight mechanisms because the ECtHR "was impressed by the interplay between the Investigatory Powers Tribunal ("IPT"), an independent body composed of persons who held or had held high judicial office and experienced lawyers which had the power, among other things, to quash interception orders, and the Interception of Communications Commissioner, likewise a functionary who held or had held high judicial office . . . and who had access to all interception warrants and applications for interception warrants").

[426] *See generally* National Defence Act, *supra* note 243, § 273.65(1).

[427] Israel, *supra* note 304, at 77.

[428] Forcese & Roach, *supra* note 424, at 12.

national security-related activities.[429] Although Parliament has the power to summon witnesses and compel testimony, it does not have a committee dedicated to national security review and, in practice, Parliamentary intervention has been sparse.[430]

Review functions rest with three bodies: the Security Intelligence Review Committee (SIRC), which oversees CSIS, the CSE Commissioner, and the RCMP Civilian Review and Complaints Commission.[431] Despite the recommendations of a public commission more than ten years ago, there is little coordination among these oversight bodies, which also suffer from shortages of resources.[432] This creates the risk that review is "stovepiped," even as the agencies maintain increasingly close levels of coordination amongst themselves.[433]

Weaknesses in the framework of *ex post* review of CSE activities are especially problematic due to the absence of prior judicial authorization. Oversight of CSE is primarily the responsibility of the CSE Commissioner, who has the authority to review classified CSE activities and internal documents and to provide independent advice to the agency and the Minister. Additionally, the CSE Commissioner's annual reports to Parliament shed light on CSE activities and offer the opportunity to enhance public dialogue. These activities serve an important function, and, as demonstrated above, past CSE Commissioners have sounded an alarm when they discovered overreach.[434]

Yet one significant weakness is that the CSE Commissioner's recommendations are not binding. Hence, the CSE Commissioner serves more as an ombudsman than as an independent body envisioned by the ECtHR, with powers to immediately terminate measures that overstep agency authority.[435] And, since the CSE Commissioner does not explain his legal reasoning in his annual report, "there is no opportunity for the

---

[429] European Parliament, Directorate-General for Internal Policies, Parliamentary Oversight of Security and Intelligence Agencies in the European Union 327 (2011), http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf.

[430] *Id.* at 319–20.

[431] Forcese & Roach, *supra* note 424, at 25–26.

[432] *Id.* at 26. *See also* Arar Commission, *supra* note 185.

[433] Forcese & Roach, *supra* note 424, at 25–26.

[434] *See supra* Part IV.B.iii.

[435] Telegraaf, App. No. 39315/06, ¶ 98.

academic or legal community to challenge these without significant guesswork or a whistle-blower."[436]

Oversight by OPC, too, fails to address these weaknesses as it is limited to review under the limited protections of the Privacy Act. Moreover, like the CSE Commissioner, OPC may issue only non-binding recommendations.[437] In sum, CSE's framework suffers from a deficiency of oversight, both in the absence of prior judicial authorization and the lack of rigorous *ex post* review sufficient to compensate for the weaknesses in its prior authorization scheme.

H. EFFECTIVE REDRESS

Finally, to meet the essentially equivalent standard, a third country must provide access to effective redress for privacy violations. Article 47 of the EU Charter guarantees "the right to an effective remedy" before "an independent and impartial tribunal."[438] In *Schrems*, the CJEU held that this right is violated where legislation does not provide "any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data."[439] The ECHR contains a similar right in Article 13.[440] In interpreting that right, the ECtHR found that the remedy does not have to be provided by "a judicial authority in the strict sense," but that "the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy is effective."[441]

Canadian federal courts have jurisdiction to hear a claim for judicial review of government action. Under its power of judicial review, a court may prohibit or restrain a government agency from an action that violates the law or the constitution.[442] This right applies to "anyone directly affected by the matter in respect of which relief is sought," not

---

[436] Israel, *supra* note 304, at 75.

[437] *Id.* at 76.

[438] EU Charter, *supra* note 22, art. 47.

[439] Schrems [2014] IEHC 310, ¶ 95.

[440] *See* ECHR, *supra* note 158, art. 13 ("Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.").

[441] Segerstedt-Wiberg and Others v. Sweden, App. No. 62332/00, Eur. Ct. H.R. ¶ 117 (2006).

[442] Federal Courts Act, R.S.C. 1985, c F-7, § 18.1(2)–(3) (Can.).

just Canadian citizens.[443] Canadian courts, therefore, are open to foreign claims, even those challenging the actions of government agencies.

One obstacle to judicial review, however, is that the targets of surveillance usually do not *know* they have been targeted. The RCMP is required to inform targets of a wiretap after its conclusion, but CSIS and CSE are under no such obligation. Even the RCMP's notification requirement does not extend in the case of access to a stored record.[444] The ECtHR makes an allowance for secrecy because it "is the very absence of knowledge of surveillance which ensures the efficacy of the interference."[445] Importantly, however, "once the measures have been divulged[,] legal remedies must become available to the individual."[446] While a foreign plaintiff likely could avail herself of a Canadian forum in a case where she had evidence that she was subjected to surveillance that violated a Canadian *statute*, her ability to make out a claim under the Canadian Charter is uncertain.[447] The absence of recourse to the Canadian Charter makes "obtaining access to justice in the national security context . . . peculiarly problematic."[448]

In Europe, even if individuals seeking to challenge a law cannot demonstrate that surveillance has been used against them, under the ECtHR's jurisprudence, they are entitled to challenge a piece of legislation if "they were members of a group of persons who were likely to be affected by measures of interception."[449] Canadian law permits such a facial challenge[450] and, unlike the United States, Canada does not have a rigid standing doctrine.[451] Under Canadian law, a court may exercise "public interest standing," which allows the court the discretion to hear a claim from a plaintiff who is not *directly* affected if there is a serious justiciable issue, the plaintiff has a genuine interest, and "the proposed

---

[443] *Id.* § 18.1(1).

[444] See Nicholas Koutros & Julien Demers, Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Law Enforcement, 11 CAN. J. L. & TECH. 79 (2013).

[445] Weber & Saravia v. Germany, No. 54934/00, Eur. Ct. H.R., ¶ 135 (2006).

[446] Segerstedt-Wiberg, App. No. 62332/00, ¶ 117.

[447] *See supra* Part IV.A.i.

[448] Jasminka Kalajdzic, Access to Justice for Wrongfully Accused in National Security Investigations, 27 WINDSOR Y.B. ACCESS TO JUST. 171, 177 (2009).

[449] Weber and Saravia v. Germany (Decision on Admissibility), App. No. 54934/00 Eur. Ct. H.R., ¶ 78 (2007).

[450] *See* Statement of Claim to the Defendant, B.C. Civil Liberties Ass'n v. Attorney Gen. of Can., T-2210-14 (2014), https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf (challenging CSE's statutory framework under the Canadian Charter).

[451] Kent Roach, The Supreme Court at the Bar of Politics: The Afghan Detainee and Omar Khadr Cases, 28 NAT'L J. CONST. L. 115, 120 (2010).

suit is a reasonable and effective way to bring the issue before the courts."[452] However, such a facial challenge may only be sustained if the plaintiff can prove that the agency acted outside its legislative mandate or that the mandate itself violated the Canadian Charter. These avenues may provide foreign plaintiffs with little comfort because of the secrecy of national security activities and the uncertain application of the Canadian Charter to the foreign surveillance.[453]

The Privacy Shield agreement addresses the absence of meaningful remedies under U.S. law through the creation of an ombudsperson with responsibility for investigating the complaints of EU residents. Under the agreement, where the ombudsperson receives a request from an EU resident that is not "frivolous, vexatious or made in bad faith," it must investigate whether the government's surveillance activities complied with US law, statutes, executive orders, presidential directives, and agency policies.[454] The ombudsperson must then confirm that the complaint was properly investigated and specify whether there was a violation of law or policy, and, if so, how it was rectified.[455] The response, however, will "neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied."[456]

Canadian law creates a similar mechanism under Section 12 of the Privacy Act, which authorizes OPC to investigate complaints against the federal government and to seek access to information held about a data subject.[457] Indeed, the role of the Privacy Commissioner in the Canadian framework has been described as an "ombudsman." Section 12, however, applies only to Canadian citizens and permanent residents, not to foreign citizens outside of Canada.[458] Although OPC has extended its policy to allow complaints from "those *in Canada* who are not

---

[452] Attorney Gen. of Can. v. Downtown Eastside Sex Workers United Against Violence Soc'y [2012] 2 SCR 524, ¶ 37.

[453] *See* Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT. SEC. L. & POLICY 179, 180-181 (2011) (finding that privacy is only weakly recognized in international human rights law and that international law is likely territorial in scope).

[454] Privacy Shield Annexes, *supra* note 171, at Annex III.

[455] *Id.* at 55.

[456] *Id.*

[457] Privacy Act, *supra* note 34, § 12(1).

[458] *Id.*

permanent residents or citizens,"[459] foreign citizens outside the country seemingly have no right to file a complaint. Given that the Article 29 Working Party was doubtful as to whether the Privacy Shield's ombudsperson would conform to the EU Charter requirements, the absence of a legal right to OPC review for foreign residents is even less likely to satisfy this standard.[460]

In some circumstances, the ECtHR has recognized that sufficient "objective supervisory machinery" can compensate for a lack of judicial recourse.[461] The threshold here is high. In *Segerstedt-Wiberg and Others v. Sweden*, the ECtHR concluded that recourse to a "Parliamentary Ombudsperson" was not a sufficient remedy because the ombudsperson could not issue a legally binding decision and did not have "specific responsibility for inquiries into secret surveillance."[462] Given the gaps in Canadian oversight discussed above,[463] and the inability of those review bodies to issue binding decisions, Canada's *ex post* review appears insufficient to meet this elevated standard.[464]

VI. CONCLUSION

Edward Snowden's revelations of NSA and global surveillance practices continue to reverberate around the world. So far, the EU-US Safe Harbor data sharing agreement was the most significant legal casualty, but it may be just the first brick to fall in a lineup of international data transfer mechanisms. The language of the *Schrems* decision makes clear that all data transfer mechanisms, and all adequacy decisions, must account for national security access to EU personal data. Under the Charter of Fundamental Rights of the European Union, as elaborated in *Schrems*, government access must be circumscribed by clear, precise, and accessible rules that are strictly necessary and proportionate to the national security interest. Additionally, there must be independent oversight and means by which EU residents can obtain effective remedies.

---

[459] *Access to Information and Privacy: Frequently Asked Questions*, OFFICE OF THE PRIVACY COMM'R OF CAN. (Feb. 17, 2014), https://www.priv.gc.ca/en/about-the-opc/opc-access-to-information-and-privacy/faqs/ (emphasis added).

[460] Data Protection Working Party, *supra* note 162.

[461] Segerstedt-Wiberg, App. No. 62332/00, ¶ 117.

[462] *Id.* ¶ 118.

[463] *See supra* Part IV.C.

[464] Penney, *supra* note 198, at 283.

This article explored the application of the *Schrems* test through the lens of the Canadian national security framework. When Canada received its adequacy decision in 2001, the European Commission did not assess government access by Canada's national security regime. In fact, national security was specifically excluded by the adequacy decision, and PIPEDA expressly allowed private entities to share data with government agencies for national security purposes. Thus, this article serves as a first review of Canada's surveillance apparatus under the newly articulated standard.

Canadian protections from foreign surveillance are vulnerable to challenge in Europe. The most significant weaknesses of the Canadian regime are the absence of clear limits to metadata access; the scope of information sharing among Canada's intelligence allies, which may allow the government to circumvent legal obligations in Canada; the absence of meaningful oversight over CSE, Canada's foreign surveillance agency; and, the difficulties of obtaining effective redress where surveillance activities are shrouded in secrecy.

There are, however, some bright spots for Canada's framework. The RCMP and CSIS must apply for a judicial warrant both to intercept private communications and to access records stored by the private sector. Moreover, the Canadian Supreme Court has positioned itself as a rigorous defender of privacy rights, at least in cases where the Canadian Charter of Rights and Freedoms applies. Finally, Canadian courts permit judicial challenges to national security surveillance, unencumbered by rigid standing doctrines.

Canada's legal framework reflects a regime designed to protect the privacy of Canadians with less regard for the privacy interests of non-Canadians outside the country. In this, the Canadian framework shares an important similarity not just with its US counterpart, but also with the national security regimes in most European countries and around the world. Thus, in Canada, and likely anywhere else, responding to the concerns of the *Schrems* decision will require a profound reorientation of the current statutory structure.

As the Canadian government moves to review national security legislation in the coming year, protections from foreign surveillance could play an important role in shaping the outcome of a future challenge to Canada's adequacy ruling. Canada could serve as a role model for assessment of the law in other countries that may face challenges to their

adequacy, including Israel and Argentina, and even the UK following its "Brexit" vote.[465] But protecting foreign privacy serves Canadians too. In an increasingly interconnected world, as information speeds through borders rendered invisible online, improving limits on foreign surveillance also protects Canadians whose data may be accessed incidentally. After *Schrems*, trade with Europe hangs in the balance.

[465] Sam Schechner, *U.K.'s EU Exit Poses Data-Protection Dilemma*, WALL ST. J. (Jun. 30, 2016), http://www.wsj.com/articles/u-k-s-eu-exit-poses-data-protection-dilemma-1467280852.