McCarthy Tétrault *Advance*™
Building Capabilities for Growth

Toronto Computer Lawyers Group: Developments in Computer, Internet and eCommerce Law: The Year in Review 2018-2019

Barry B. Sookman
bsookman@mccarthy.ca
416-601-7949

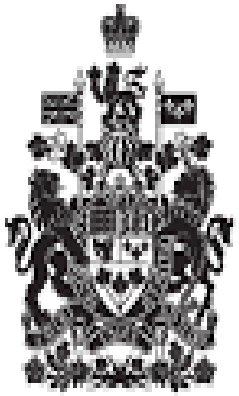
June 13, 2019

Overview

- Privacy / Big Data / AI
- Employee / HR
- E-commerce / Online Agreements
- Online Remedies / Governance / Jurisdiction
- Copyright

Privacy/Big Data/AI

PIPEDA Report of Findings #2019-001 - Equifax



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Does a transfer of personal information require consent?

- Prior OPC guidance:
  - OPC Processing Personal Data Across Borders Guidelines, January 2009 (*OPC Cross Border Guideline*)
  - PIPEDA Case Summary #2005-313
  - PIPEDA Case Summary #2008-394
- Transfer for processing is a “use” and not a disclosure. No new consent is required.
- Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities.

Does a transfer of personal information require consent?

- "Equifax Inc. … received credit reporting information transferred to it by Equifax Canada about those consumers to fulfil those products. Also as described in Section 3 of this report, Equifax Canada remained accountable for this information transferred to Equifax Inc. for processing, and responsible for the related obligations under PIPEDA 4.1.3.
- At the same time, these transfers for processing from Equifax Canada to Equifax Inc. constitute disclosures of personal information under the meaning of PIPEDA Sections 7(3), and 4.3."
- "…we acknowledge that in previous guidance our Office has characterized transfers for processing as a 'use' of personal information rather than a disclosure of personal information. Our guidance has also previously indicated that such transfers did not, in and of themselves, require consent. In this context, we determined that Equifax Canada was acting in good faith in not seeking express consent for these disclosures."

Does a transfer of personal information require consent?

- OPC Consultation on transborder dataflows and supplementary discussion document (a transfer is a disclosure)
- Government of Canada Proposals to modernize the Personal Information Protection and Electronic Documents Act (a transfer is a disclosure but consent may not be needed)
- OPC Consultation on transfers for processing – Reframed discussion document
- "To be clear, we would not recommend that consent be required in the longer term in the context of data transfers for processing, if other effective means are found to protect the privacy rights of individuals. But in situations where neither contractual clauses nor other means are effective, consent may be required."
- "The change in position by the OPC would require organizations to highlight elements that were previously part of their openness obligations and ensure that individuals are aware of them when obtaining consent for transborder transfers. We are open to views on how (implied or express consent, content of the information upon which consent would be sought) this might be achieved".

Accountability principle

"PIPEDA Principle 1 – Accountability, states, that an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. Further, Section 4.1.3, states that an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

Accountability principle

- OPC Cross Border Guideline:
- “As the principle suggests, the primary means by which an organization may protect personal information that is sent to a third party for processing is through a contract.
- Regardless of where the information is being processed - whether in Canada or in a foreign country - the organization must take all reasonable steps to protect it from unauthorized uses and disclosures while it is in the hands of the third party processor. The organization must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times. It should also have the right to audit and inspect how the third party handles and stores personal information, and exercise the right to audit and inspect when warranted.”

Accountability principle

- “In relation to this analysis, we note that the overarching Accountability Principle states, in Section 4.1, that an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the PIPEDA principles. It is therefore a key aspect of accountability that the individual designated by the organization, in this case, Equifax Canada’s CPO, must have tools and structures in place to enable him or her to be truly accountable for the handling of personal information.
- In this context we examined the nature of the controls put in place by Equifax Canada, including the role of its CPO, to ensure that Canadian personal information processed by Equifax Inc. receives a level of protection comparable to that required under PIPEDA.
- To determine the appropriate level of controls, consideration must be given to both the scope and sensitivity of personal information being handled. In some cases where the third party is closely affiliated and the personal information being handled is of limited scope and sensitivity, it may be possible to rely on light controls and pre-existing, adequate, policies and practices of the third party to fulfil the obligations under 4.1.3”

Accountability principle

- "In a case where a substantial volume of sensitive personal information belonging to a large number of individuals is being handled over a prolonged period, the level of controls should be commensurately high. In such a situation, in our view, PIPEDA Principle 4.1.3 requires, at a minimum:
- a. A formal written arrangement, updated periodically and in the case of material changes, which should generally include details about the following:
  - what personal information is being handled by the third party, including both information shared by the organization and any information collected directly by the third party on behalf of the organization;
  - what specific rules, regulations and standards need to be complied with in the handling of the information, including PIPEDA;
  - the roles and responsibilities of key stakeholders within both organizations for the handling of the personal information, including responsibilities for specific functions, decision-making, safeguards and breach response;
  - information security obligations;
  - acceptable uses of the information;
  - retention and destruction obligations; and
  - reporting and oversight arrangements to ensure compliance with the above, including reporting obligations in the case of a breach that could compromise the personal information.

Accountability principle

- b. A structured program for monitoring compliance against the obligations laid out in the arrangement. The program should be suitable to the scope and sensitivity of the personal information being handled. It should include:
  - mechanisms for periodic reporting by the third party on the handling of the personal information; and,
  - where scope and sensitivity of the personal information handled is significant, mechanisms to ensure periodic external assessment (by the organization or an appropriate third party) of compliance with the full range of obligations described in the written arrangement.
- When a third party is handling personal information for an organization, it is important that the organization have measures in place to periodically ensure that the third party is actually fulfilling its obligations to protect that personal information. This could include reviewing reporting from the third party on information handling, third party audits or certifications against clearly laid out obligations, or direct oversight of the third party on a periodic basis. Where, as in this case, the third party is continuously processing a significant volume of sensitive personal information, these measures must be commensurately robust. Such measures can be used by the designated Privacy Officer to ensure they fulfil their accountability role wherever information is held.

Accountability principle

- "In our view, it would generally be reasonable, for the purpose of assessing a third party's compliance with PIPEDA's safeguards requirements, for an organization to rely on an up-to-date security certification conducted under the following conditions: (i) by an appropriate party, (ii) against an appropriate security standard, and (iii) in the absence of contradictory indicators of security concerns.
- The standard used in this case, ISO 27001, is appropriate, as it is specific to information security, comprehensive, peer reviewed, regularly updated, and broadly recognized….
- However, in this case, Equifax Canada was also privy to other information about Equifax Inc.'s security practices which clearly cast doubt as to whether Equifax Inc. remained ISO 27001 compliant…
- In the context of this additional knowledge by Equifax Canada, it was therefore not reasonable for it to rely on the ISO 27001 certification as assurance of adequate security by Equifax Inc. Cognizant of such poor practices, Equifax Canada should have taken further measures to assess the security of Canadian personal information held by Equifax Inc. and ensure that any necessary corrective measures were taken in a timely way."

Processor independent PIPEDA obligations

- "Equifax Inc.'s safeguards were lacking in the following four areas:
  - vulnerability management;
  - network segregation;
  - implementation of basic information security practices; and
  - oversight.
- In our view, the specific weaknesses described above individually and collectively constitute failures to implement appropriate security safeguards given the volume and sensitivity of the personal information held by Equifax Inc. Consequently, in relation to the safeguards of personal information by Equifax Inc., the matter is **well-founded**."

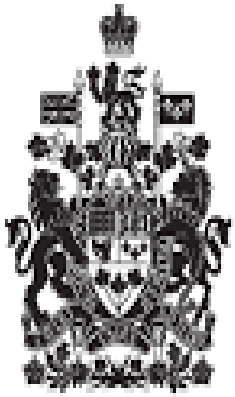
Internal security safeguards

- Under the PIPEDA Safeguards Principle (4.7)…personal information must be protected by security safeguards appropriate to the sensitivity of the information.
- For an organization protecting significant volumes of sensitive personal information, as is the case for Equifax Canada, in our view the following high level oversight mechanisms, or alternative equivalent measures, would be required under PIPEDA's safeguards principle:
  - at least annually, a comprehensive internal assessment of the full security program, and at least every two years, a comprehensive external security audit;
  - regular internal and external penetration testing (frequency based on context, including risk assessment and complexity), including comprehensive external penetration testing at least annually.

Internal security safeguards

- “Fundamentally, penetration testing is an authorized simulated attack on an organization’s systems and is used to evaluate the security of the system… The internal penetration testing specific to Equifax Canada at the time of the breach had two major deficiencies:
  - It should have been conducted more often than once a year considering the context, which included a high volume of sensitive information and risks identified; and
  - It did not include basic, necessary components of penetration testing. The testing conducted did not include the use of any exploitation tools used by attackers, and overall, employed a very limited menu of tools and techniques…”

PIPEDA Report of Findings #2019-002 (Facebook)



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Consent for TYDL (this is your digital life)

- "…in our view, when Facebook provides third party applications with access to personal information under its control via its Graph API, this constitutes a disclosure by Facebook. Accordingly, under PIPEDA, Facebook is required to ensure knowledge and meaningful consent for that disclosure…
- "In order for consent to be considered meaningful, organisations must inform individuals of their privacy practices in a clear, comprehensive and understandable manner. The provision of this information should be presented in a timely manner, such that users have the relevant information and context needed to make an informed decision before or at the time when their personal information is collected, used or disclosed. As of June 2015, PIPEDA also stipulates that consent of individuals is only valid if it is reasonable to expect the individual would understand the nature, purposes and consequences of the collection, use or disclosure of personal information to which they are consenting."

Consent for TYDL APP from installing users – direct by FB

- Facebook asserts that all Facebook users must agree to terms and conditions when they register their account. These terms and conditions were set out in two public-facing policies, then-titled Statement of Rights and Responsibilities ("SRR") and Data Use Policy ("DP").
- The DP: ""Controlling what information you share with applications […]When you connect with a game, application or website – such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline – we give the game, application, or website (sometimes referred to as just "applications" or "apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info."

Consent for TYDL APP from installing users – consent via Apps

- SRR: “When you [user] use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. ***We [Facebook] require applications to respect your privacy***, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.)”
- “Facebook relies on apps to obtain consent from Installing Users for the disclosure of users’ personal information to the app. During the relevant period, Facebook maintained that, prior to an app being installed, Installing Users would have been presented with an app-installation dialog box which provided information about the categories of information the app would receive if installed, and a link to a privacy policy for the app. Facebook asserts that this would have been the case for the TYDL App.”

Consent for TYDL APP from installing users – direct by FB

"… we are of the view that the language in the … DP (Data use Policy), itself, would have been too broad to be relied upon as meaningful consent for disclosures of personal information to the TYDL App. Even if the user had actually found and read the relevant language in these documents, which total 4500 and 9100 words in length, respectively, these documents did not highlight the purposes for which Facebook would have disclosed a user's personal information to the TYDL App, or the potential consequences of such a disclosure."

Consent for TYDL APP from installing users – consent via Apps

"We have previously found that organisations may rely, in appropriate circumstances, on consent obtained by third party organisations. However, the organization relying on consent obtained by the third party should take reasonable measures to ensure the third party is actually obtaining meaningful consent. The organization relying on consent obtained by the third party is still ultimately responsible for meeting its obligations under the Act."

Consent for TYDL APP from installing users – consent via Apps

"Facebook relied on apps to obtain consent from users for its disclosures to those apps, but Facebook was unable to demonstrate that: (a) the TYDL App actually obtained meaningful consent for its purposes, including potentially, political purposes; or (b) Facebook made reasonable efforts, in particular by reviewing privacy communications, to ensure that the TYDL App, and apps in general, were obtaining meaningful consent from users."

"Facebook did not implement this model in a way that ensured meaningful consent. In particular, Facebook did not check that the "operable link" displayed during installation led to a document that explained the app's privacy practices, nor that those explanations were sufficient to support meaningful consent for Facebook's disclosure of users' information to the app. A framework or general approach cannot produce real protection unless it is accompanied by meaningful information to the users whose personal information is to be disclosed."

Facebook's safeguard obligations against unauthorized access, use and disclosure

- **What obligations does a controller have after a disclosure of personal information?**
- "Facebook's Platform Policy required the TYDL App to: only request the data it needed to operate the TYDL App, not transfer data to third parties, and not use the data outside of the application. The Platform Policy also required… "subject to certain restrictions, including on use and transfer, users give [apps] their basic account information when they connect with [app developer's] application. For all other data obtained through use of the Facebook API, [app developer] must obtain explicit consent from the user who provided the data to us before using it for any purpose other than displaying it back to the user on [app developer's] application.""
- "there was an unauthorized access and use of Facebook users' personal information. The question at hand is whether Facebook had adequate safeguards in place to protect against this."

Facebook's safeguard obligations

- "Facebook did not have adequate proactive monitoring, or enforcement, of apps' compliance with the Platform Policy. Other than for "Top Apps", Facebook relied too heavily on inadequate reactive measures. While Graph v.2 and App Review represent a safeguards improvement, in that they are proactive measures to protect against apps' unauthorized access to users' information, Facebook has provided insufficient evidence that its ongoing monitoring and enforcement adequately safeguards users' information against unauthorized use or onward disclosure, after the one-time App Review process."
- "However, for the more than 300,000 apps which Facebook granted extended permissions, these measures do nothing to ensure ongoing compliance with respect to third-party apps' use and disclosure of user data for which Facebook has approved that access. For example, they do not ensure the app uses the information in a manner that is consistent with the app's representations to Facebook during App review, or with Facebook's policies."

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V. Case C-40/17 (Advocate General Opinion)

- **Whether a person that transfers personal data via a plug-in to a social network (Facebook) is a joint controller responsible for all uses of the personal data by the social network.**
- "Will effective protection be enhanced if everyone is made responsible for ensuring it?
- That, in a nutshell, is the deeper moral and practical dilemma demonstrated by the present case and expressed in legal terms by the scope of the definition of (joint) controller. In the understandable desire to secure the effective protection of personal data, the recent case-law of the Court has been very inclusive when being asked to define, in one way or another, the notion of (joint) controller. So far, however, the Court has not been faced with the practical implications of such a sweeping definitional approach with regard to the subsequent steps of exact duties and specific liability of parties who are classified as joint controllers."

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V. Case C-40/17 (Advocate General Opinion)

- "there ought to be, perhaps not always an exact match, but at least a reasonable correlation between power, control, and responsibility. Modern law naturally includes various forms of objective liability, which will be triggered merely by certain results occurring. But those tend to be justified exceptions. If, without any reasoned explanation, responsibility is attributed to someone who had no control over the result, such allocation of liability will typically be seen as unreasonable or unjust…
- Finally, no good (interpretation of the) law should reach a result in which the obligations provided therein cannot actually be carried out by its addressees. Thus, unless the robust definition of (joint) control is not supposed to turn into a judicially sponsored command to disconnect which is applicable to all actors, and to refrain from using any social networks, plug-ins, and potentially other third-party content for that matter, then in defining the obligations and responsibilities, reality must play a role, again including issues of knowledge and genuine bargaining power and the ability to influence any of the imputed activities."

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V. Case C-40/17 (Advocate General Opinion)

- "On the facts in the present case, it thus appears that the Defendant and Facebook Ireland co-decide on the means and purposes of the data processing at the stage of the collection and transmission of the personal data at issue. To that extent, the Defendant acts as a controller and its liability is, to that extent as well, joint with that of Facebook Ireland.
- At the same time, I consider that the liability of the Defendant has to be limited to the stage of the data processing, in which it is engaged and that it cannot spill over into any potential subsequent stages of data processing, if such processing occurs outside the control and, it would appear, also without the knowledge of the Defendant.
- In the light of the above, my second interim conclusion is therefore that a person, such as the Defendant, that has embedded a third-party plug-in in its website, which causes the collection and transmission of the user's personal data (that third party having provided the plug-in), shall be considered to be a controller within the meaning of Article 2(d) of Directive 95/46. However, that controller's (joint) responsibility is limited to those operations for which it effectively co-decides on the means and purposes of the processing of the personal data."

Reference re subsection 18.3(1) of the Federal Courts Act, R.S.C. 1985, c. F-7, 2019 FC 261 (Google right to be forgotten)

- The Privacy Commissioner has chosen to refer only those two jurisdictional issues to the Court and in its Notice of Application, has formulated the reference questions as follows:
  - (1) Does Google, in the operation of its search engine service, collect, use or disclose personal information in the course of commercial activities within the meaning of paragraph 4(1)(a) of PIPEDA when it indexes webpages and presents search results in response to searches of an individual's name?
  - (2) Is the operation of Google's search engine service excluded from the application of Part I of PIPEDA by virtue of paragraph 4(2)(c) of PIPEDA because it involves the collection, use or disclosure of personal information for journalistic, artistic or literary purposes and for no other purpose?

Reference re subsection 18.3(1) of the Federal Courts Act, R.S.C. 1985, c. F-7, 2019 FC 261

- "The Court accepts that the determination of the issues on this reference may require consideration of the *Charter*. Indeed, the Court must ensure that it interprets the provisions of *PIPEDA* that are at issue in a manner that respects rather than offends constitutionally protected rights. That said, there is a difference between using the Charter as an aid to statutory interpretation and using it to challenge the applicability or validity of the statute. The reference questions as framed contemplate the consideration of the Charter in the interpretation of s 4(1)(a) and 4(2)(c) of PIPEDA, but does not include the determination of whether, when properly interpreted, their application would contravene the *Charter*."
- **OPC also not asking the Court to determine whether there is a right to be forgotten or if such a right would offend the *Charter*.**

Privacy Class Actions

- Broutzas v. Rouge Valley Health System, 2018 ONSC 6315 (hospital employees accessing PHI and disclosing contact information used to sell RESPs; not certified failing common issues and preferable procedures criterion; claims under s65 OHIPA, negligence (against some of the defendants) recognized; rejection of claim of intrusion on seclusion as there was intrusion by not "on seclusion".)
- Kaplan v. Casino Rama, 2019 ONSC 2025 (hacker posts PI of 11,000 people online after cyber attack; not certified failing common issue criterion; claims for neglience, breach of contract and intrusión upon seclusion recognized.)
- Tocco v. Bell Mobility Inc., 2019 ONSC 2916 (alleged use of PI for relevant advertising program (RAP) based on findings of OPC certified based on numerous causes of action including breach of contract, negligence, intrusion upon seclusion, breach of Consumer Protection Act).

British Columbia v. Philip Morris International, Inc., [2018] 2 SCR 595

- HMTQ v. Philip Morris International, Inc., 2017 BCCA 69 "Once stripped of personal identifiers, disclosure of the anonymized data poses no realistic threat to personal privacy." Reversed.
- "Unlike the courts below, however, I would reject Philip Morris's submission that simply because the databases, due to their aggregate nature, may be of a "very different character" than original clinical records, they must therefore fall outside of the protective scope of s. 2(5)(b). As already shown, the databases are both "records" and "documents" within the meaning of the Act. They store the health care information of particular individual insured persons. And, while that information is stored on an aggregate rather than individual basis, each data entry in the databases is derived from particular individuals' clinical records. The mere alteration of the method by which that health care information is stored — that is, by compiling it from individual clinical records into aggregate databases — does not change the nature of the information itself. Even in an aggregate form, the databases, to the extent that they contain information drawn from individuals' clinical records, remain "health care records and documents of particular individual insured persons"."

OSFI Technology and Cyber Security Incident Reporting (effective Mar. 2019)

- "For the purpose of this Advisory, a technology or cyber security incident is defined to have the potential to, or has been assessed to, materially impact the normal operations of a FRFI, including confidentiality, integrity or availability of its systems and information."
- "Technology or Cyber Security Incidents assessed by a FRFI to be of a high or critical severity level should be reported to OSFI."
- Includes:
  - Criteria for Reporting
  - Initial Notification Requirements
  - Subsequent Reporting Requirements
  - Appendix which provides some examples of reportable incidents.

Canada's Digital Charter

California Consumer Privacy Act of 2018

- Gives consumers right to learn categories of personal information that businesses collect, sell, or disclose about them, and to whom information is sold or disclosed.
- Gives consumers right to prevent businesses from selling or disclosing their personal information.
- Prohibits businesses from discriminating against consumers who exercise these rights.
- Allows consumers to sue businesses for security breaches of consumers' data, even if consumers cannot prove injury.
- Allows for enforcement by consumers, whistleblowers, or public agencies. Imposes civil penalties.
- Applies to online and brick-and-mortar businesses that meet specific criteria. AG California Summary, Dec. 18, 2017.

Canada Directive on Automated Decision-Making (effective April 1, 2019)

- "The objective of this Directive is to ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian law."
- See, Risk Management Framework in Appendices.
  - See also,
    - Singapore A proposed Model Artificial Intelligence Governance Framework, January 2019
    - EU Commission High Level Expert Group on AI, Ethics Guidelines for Trustworthy AI (April 2019)
    - Artificial Intelligence: Australia's Ethics Framework (April 2019)
    - OECD Council Recommendation on Artificial Intelligence (May 2019)
    - ITECHLAW: Responsible AI: A Global Policy Framework (May 2019)

Canada Directive on Automated Decision-Making

Access to components

- If using a proprietary license, ensuring that:
  - All released versions of proprietary software components used for Automated Decision Systems are delivered to, and safeguarded by, the department.
  - The Government of Canada retains the right to access and test the Automated Decision System, including all released versions of proprietary software components, in case it is necessary for a specific audit, investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.
  - As part of this access, the Government of Canada retains the right to authorize external parties to review and audit these components as necessary.
- Release of source codes.

Kahn v. Upper Grand District School Board, 2019 HRTO 863

- **Does raw data to a psychological testing tool have to be produced to enable expert analysis to determine discrimination based in disability?**
- "The issue of whether psychologists should be required to disclose raw data from copyrighted assessment tools has been considered in the courts…The existence of the two competing interests that arise in this situation was succinctly described in *Asrat v. 1438305 Ontario Inc., et al*, 2017 ONSC 3801 (CanLII) as follows (at paragraph 8):
  - The first is the public interest in having all relevant evidence before the Court. In that regard, Justice Edwards [in *Long et al. v. Dundee Resort et al*., 2012 ONSC 3202 (CanLII)] discussed the importance of counsel having the raw data once the action had reached the pre-trial stage such that he could prepare for cross-examination of the opposing party's expert. Second, there is a legitimate interest of psychologists in maintaining the integrity and validity of the mental health process"".

CASL – Charter Challenge

Employee/HR

Sprint Electric Ltd v Buyer's Dream Ltd [2018] EWHC 1924 (Ch) (30 July 2018)

- "With regard to the express terms of the 1997 Contract, SEL contends that the combined effects of Clauses 4.1 and 4.2 required BDL to make the Source Code and related Documents available to it. In the 1997 Contract, "Sprint's Business" is defined as SEL's "business of motion control". Clause 4 of the 1997 Contract is entitled "DEVELOPMENT OF BUSINESS" and provides as follows:
  - "BDL undertakes that it shall:
  - *4. 1 Use its best endeavours to develop Sprint's Business to its full potential in the most economic efficient and profitable way with best business practice*
  - *4. 2 Disclose all material information concerning the running of Sprint's Business."*

Sprint Electric Ltd v Buyer's Dream Ltd [2018] EWHC 1924 (Ch) (30 July 2018)

- "Pulling all these strands together, and having considered these matters for the reasons set out above and in spite of the fact that none of the parties argued that the 1997 Contract did not correctly describe the true relationship pursuant to which SEL obtained the benefit of his personal services, I have come to the conclusion that the true relationship between SEL and Dr Potamianos under the 1997 Contract was that of employer and employee."
- "In reaching that conclusion, I have paid careful regard to the submissions of BDL and Dr Potamianos to the effect that the only permissible approach for the Court is to construe the relevant terms of (among others) the 1997 Contract and identify its objective meaning, that the parties have to live with the contractual structures that they have chosen to adopt, that it is not legitimate for the Court to "look through" a structure or to infer that a contractor should simply be treated as if he were an employee, and that I should heed Lord Neuberger PSC's precautionary observation that: "Concentrating on the perceived morality of the parties' behaviour can lead to an unacceptable degree of uncertainty of outcome" (Thornton v Major [2009] 1 WLR 776, at [98])."
- "On that basis, and as there was no agreement to the contrary, SEL was and is the owner of the copyright in the documents and the source code which were authored by Dr Potamianos under the 1997 Contract, in accordance with section 11(2) of the CDPA."

Sprint Electric Ltd v Buyer's Dream Ltd [2018] EWHC 1924 (Ch) (30 July 2018)

- In the alternative: "I consider that the reasoning in *Griggs v Evans* applies to the present case. A contract under which SEL agreed not only that it should pay for the creation of the Source Code and Related Documents but also that it should be denied ownership of, or even any right of access to, those materials, and be confined instead to a right to exploit the Object Code, is one which no reasonable persons in the position of SEL and Dr Potamianos would have made, and which lacks commercial and practical coherence. So far as concerns the nature and extent of the appropriate implied grant of rights, I consider that this case falls within principle (7) identified by Lightman J in [*Robin Ray v Classic FM plc* [1998] FSR 622].
- ["circumstances may exist when the necessity for an assignment of copyright may be established…..]
- "For these reasons, I consider that the implied term of the 1997 Contract for which SEL contends, namely an implied term that BDL and Dr Potamianos have at all material times been obliged to provide SEL with "the Source Code and Documents" as defined in paragraph 57 of the Particulars of Claim to the extent that the same were created by Dr Potamianos during the existence of the 1997 Contract satisfies the conditions that (1) it is reasonable and equitable; (2) it is necessary to give business efficacy to the contract; (3) it is so obvious that "it goes without saying"; (4) it is capable of clear expression; and (5) it does not contradict any express term of the contract."

Sprint Electric Ltd v Buyer's Dream Ltd [2018] EWHC 1924 (Ch) (30 July 2018)

"In cases, like the present, which relate to events which happened over many years, in which feelings run high, and in which individuals have taken up entrenched positions in their written evidence by the time the case comes to trial, there are significant risks that witnesses may be honest but mistaken about what took place, and may give evidence about what they would like to think happened rather than what they can truly recollect. These factors make the appraisal of their evidence more difficult. At the end of the day, the best guide to the truth is often to be found not so much in the demeanour of the protagonists, or even concessions made in cross-examination, but in the contemporary documents and in an objective appraisal of the probabilities overall."

M.W. v Samsom Industries Ltd., 2019 CanLII 48076 (MB LB)

- **Is a refusal to provide a password to an employee/bookkeeper's computer which leaves the company in a difficult position just cause for dismissal?**
- "The seminal case on the modern concept of just cause is found in the dissenting opinion of Schroeder, J.A. in *R.* v. *Arthurs*, *Ex parte Port Arthur Shipbuilding Co*., (1967), 1967 CanLII 30 (ON CA), 62 D.L.R. (2d) 342 (Ont. C.A.) rev'd 1968 CanLII 29 (SCC), [1969] S.C.R. 85:
  - If an employee has been guilty of serious misconduct, habitual neglect of duty, incompetence, or conduct incompatible with his duties, or prejudicial to the employer's business, or if he has been guilty of willful disobedience to the employer's orders in a matter of substance, the law recognizes the employer's right summarily to dismiss the delinquent employee."

M.W. v Samsom Industries Ltd., 2019 CanLII 48076 (MB LB)

"The determination for this Board is whether the Employee's conduct is sufficiently serious that it would give rise to a breakdown in the employment relationship. Having regard to all of the circumstances, the Board is not convinced that the Employer's response to terminate was proportional to the Employee's actions, specifically in light of the Board's finding that theft was not established by the Employer. Accordingly, the Employer has not satisfied the Board that the employment of the Employee was terminated for just cause and, therefore, the Employee is entitled to the wages in lieu of notice as provided for in this Order."

Menard v. The Centre for International Governance Innovation, 2019 ONSC 858

- **Is using P2P software to share copyright content (60 GB) and copying documents to bring home contrary to employer policies grounds for dismissal for cause?**
- "With respect to the use of peer-to-peer software and downloading material, at the end of the day this does not constitute cause for dismissal without notice.
- At most, CIGI can show that this activity violated one or more internal policies of CIGI. There was no nefarious intent on Mr. Menard's part, and indeed he made no attempt to hide what he was doing. He testified, without contradiction, that someone from the IT department assisted him in installing the peer-to-peer software. When Mr. Miller discovered, in a limited way, that some peer-to-peer software was being used, Mr. Miller did not report it to anyone or take any other action. I am not suggesting that Mr. Miller was in any position to condone the activity, but the fact that Mr. Menard made no attempt to hide the activity from Mr. Miller demonstrates, in my view, that he did not think he was doing anything improper."

Menard v. The Centre for International Governance Innovation, 2019 ONSC 858

- "While I accept, with some reservations, Mr. Menard's evidence that he did not know that copyright material was being downloaded, I think his evidence should be taken with a grain of salt. Any reasonable person would likely agree, if asked, that there is copyright in a current television program such as "Game of Thrones". Any reasonable person would know that one can purchase, in electronic form, a movie, a television program, or music, and if one can obtain it through computer software without paying for it there is likely a problem.
- However, it is well known that this sort of software is ubiquitous, and indeed Mr. Miller acknowledged that he had used it himself on his home computer….
- I agree with Mr. Monkhouse that if Mr. Menard had been spoken to about using peer-to-peer software on his computer and keeping corporate documents at home, there is little doubt that Mr. Menard would have complied. I am not persuaded that Mr. Menard's delinquencies were incompatible with a continuation of the employment relationship."

e-Commerce & Online Agreements

TELUS Communications Inc. v. Wellman, 2019 SCC 19

- **Does s7(5) of the Arbitrations Act grant the court a discretion to refuse to stay non-consumer claims that are dealt with in an arbitration agreement?**
- "while my colleagues maintain that the Act was designed with "freely negotiat[ed]" arbitration agreements in mind, nothing in the Arbitration Act suggests that standard form arbitration agreements, which are characterized by an absence of meaningful negotiation, are per se unenforceable. Indeed, this Court's decision in *Seidel* — as well as its predecessors *Dell, Rogers, and Desputeaux* — confirm that the starting presumption is the opposite."
- "…in the years since the *Arbitration Act* was passed, the jurisprudence — both from this Court and from the courts of Ontario — has consistently reaffirmed that courts must show due respect for arbitration agreements and arbitration more broadly, particularly in the commercial setting...In *Seidel*, Binnie J. noted that "[t]he virtues of commercial arbitration have been recognized and indeed welcomed by our Court" (para. 23), and he stated that "absent legislative language to the contrary" (para. 42 (emphasis deleted)), "the courts will generally give effect to the terms of a commercial contract freely entered into, even a contract of adhesion, including an arbitration clause"."

TELUS Communications Inc. v. Wellman, 2019 SCC 19

- "The legislature made a careful policy choice to exempt consumers — and only consumers — from the ordinary enforcement of arbitration agreements. That choice must be respected, not undermined by reading s. 7(5) in a way that permits courts to treat consumers and non-consumers as one and the same."
- "Furthermore, Mr. Wellman has not argued, either before this Court or the courts below, that the standard form arbitration agreement in question was unconscionable, which if proven would render it invalid and thereby provide a basis for refusing a stay pursuant to s. 7(2)2 of the *Arbitration Act*. In my view, arguments over any potential unfairness resulting from the enforcement of arbitration clauses contained in standard form contracts are better dealt with directly through the doctrine of unconscionability, which was the approach taken in *Heller v. Uber Technologies Inc*., 2019 ONCA 1, rather than indirectly by attempting to stretch the language of s. 7(5) to address a perceived problem it was never designed to address."

Heller v. Uber Technologies Inc., 2019 ONCA 1, leave to Supreme Court granted, Case 38534

- **Whether mandatory mediation/arbitration agreement with drivers is unconscionable?**
- ONCA accepts that click-wrap would otherwise be enforceable:
  - "The first time a driver logs into the Uber App, he or she must accept a services agreement, which appears on the smartphone screen. Drivers accept by clicking "YES, I AGREE", and confirming acceptance by again clicking "YES, I AGREE" after reading the following: "PLEASE CONFIRM THAT YOU HAVE REVIEWED ALL THE DOCUMENTS AND AGREE TO ALL THE NEW CONTRACTS." Uber's January 4, 2016 Driver service agreement with the appellant is 14 pages. The November 29, 2016 UberEATS service agreement with the appellant is 15 pages."

Heller v. Uber Technologies Inc., 2019 ONCA 1, leave to Supreme Court, Case 38534

"In approaching that issue, I start with the approach taken by the majority in *Douez*. While I recognize that the clause in question in *Douez* was a forum selection clause, I see no reason in principle why the same approach ought not to be taken to the Arbitration Clause in this case. I say that because the Arbitration Clause here is not, strictly speaking, simply an arbitration provision. It is also a forum selection provision and it is a choice of laws provision. It covers much more than just the method through which disputes will be resolved. It establishes both a foreign forum for the adjudication and a foreign law that will be applied in that adjudication. Consequently, the Arbitration Clause should be subject to a broader analysis when it comes to the issue of validity, especially in a situation where it is part of a contract of adhesion."

Heller v. Uber Technologies Inc., 2019 ONCA 1, leave to Supreme Court, Case 38534

- " I find that the Arbitration Clause is unconscionable when it is viewed properly and in the context in which it is intended to apply."
- "It seems to me that the fundamental flaw in the approach adopted by the motion judge to this issue is to proceed on the basis that the Arbitration Clause is of the type involved in normal commercial contracts where the parties are of relatively equal sophistication and strength. That is not this case. As the majority in *Douez* noted, "forum selection clauses often operate to defeat consumer claims" (para. 62). The same can be said of the Arbitration Clause here – it operates to defeat the very claims it purports to resolve. And I reiterate that this Arbitration Clause is much more than just a simple arbitration provision."

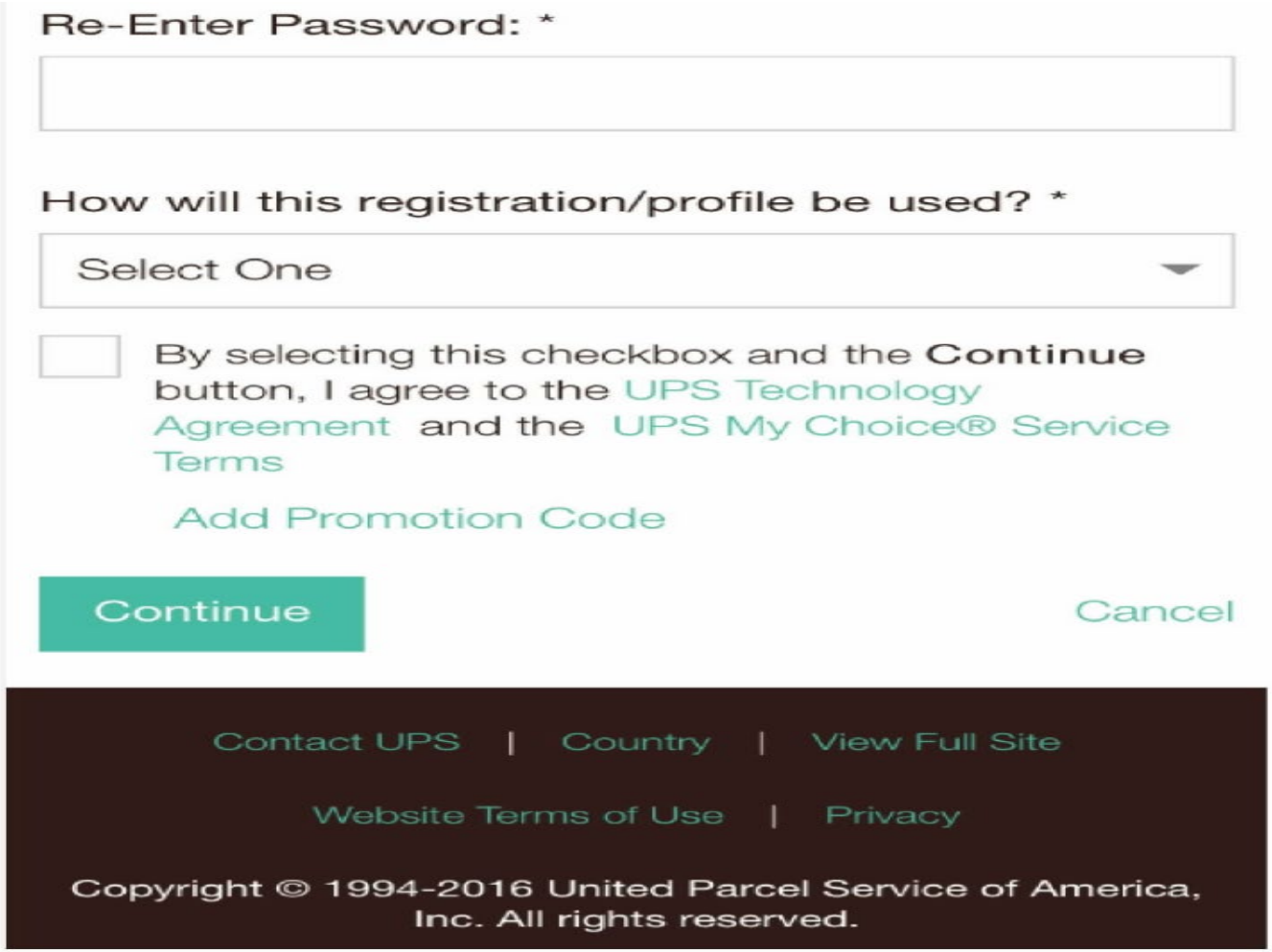
WCL Capital Group Inc. v. Google LLC, 2019 ONSC 947

- “I accept Google’s submission that the forum selection clause is enforceable and applicable to the present case. The Terms of Service were written in plain language and were accepted by WCL. The forum selection clause requires the parties to resolve in California any claims "arising out of or relating to" the agreement.
- WCL did not argue that forum selection clause is not applicable because WCL also seeks to claim negligence and negligent misrepresentation against Google. As Google submits, forum selection clauses like this one have been found to apply to non-contractual claims, so long as they relate to a relationship arising from contract. Courts must assess the "essential character" of the dispute to determine whether the forum selection clause applies. As submitted by Google, the essential character of this claim is in contract.
- WCL also argued that the forum selection clause is not applicable to its claim because it alleges Google engaged in deceitful conduct in mischaracterizing the nature of WCL’s dispute in order to secure a reversal of the credit which had been applied to WCL’s Amex card. I see no reason why this allegation is not part of WCL’s claim, caught by the forum selection clause.”

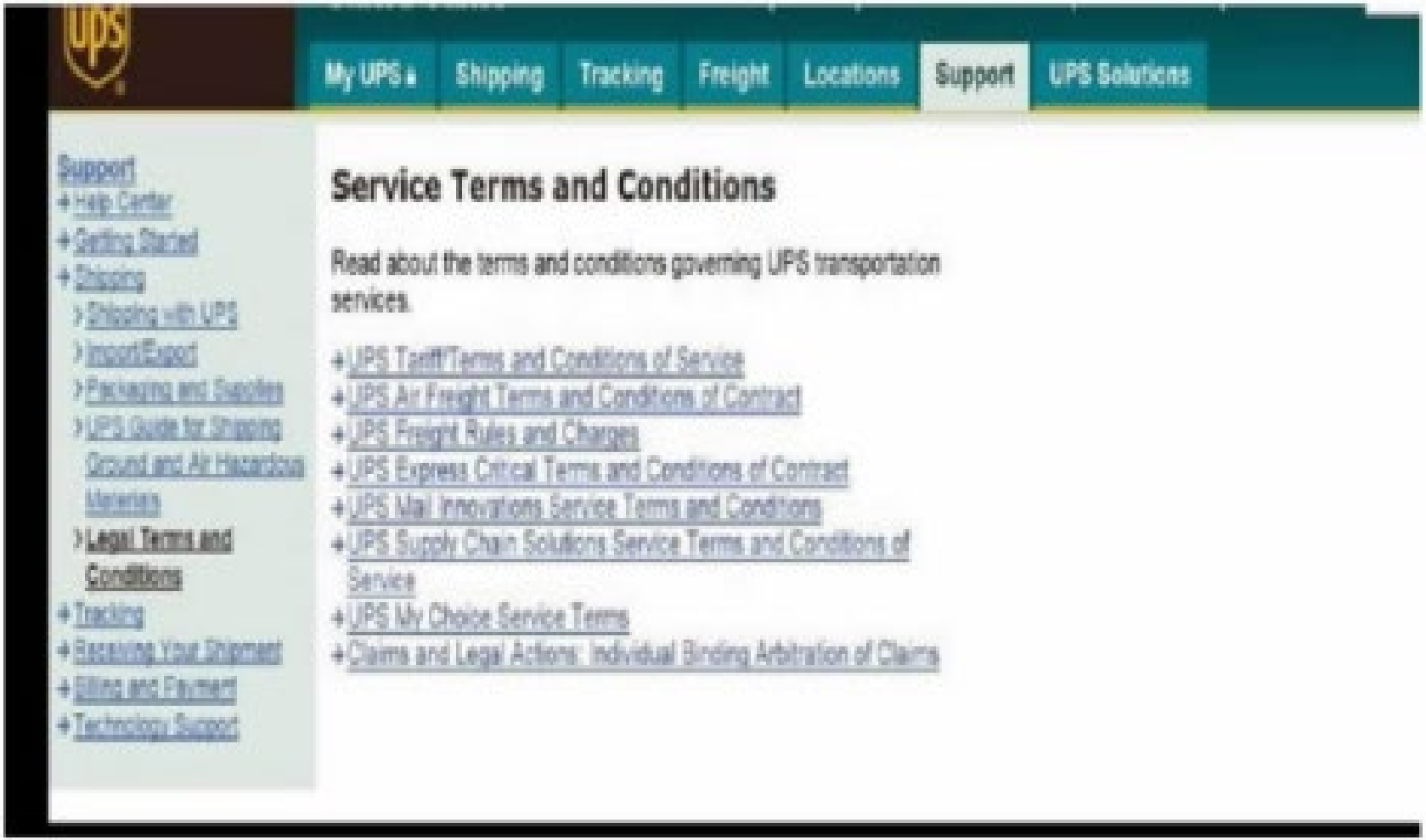
WCL Capital Group Inc. v. Google LLC, 2019 ONSC 947

- "WCL submits that the importance of WCL's claim to Ontario arises from the fact its claim arises from a flaw in an algorithm in Google's software which, in 2016, delivered $2.614 billion in online advertising on behalf of Canadian businesses which is relevant to all persons in Ontario. This is especially the case here where the flaw resulted in the delivery of advertising to children, who were not the intended audience. WCL argues that this is a matter of the public interest, which should not be handed over to the courts in California….
- In my view the WCL claim has significantly less of a public dimension, involving an advertising agreement between two commercial parties. There is no public policy reason why it should not be decided in California. In fact, a decision there would arguably have a much larger impact on businesses from all countries, including Canadian corporations using this type of advertising."

IN RE Randall HOLL, 2019 WL 2293441 (9th.Cir.May 30, 2019)



IN RE Randall HOLL, 2019 WL 2293441 (9th.Cir.May 30, 2019)



IN RE Randall HOLL, 2019 WL 2293441 (9th.Cir.May 30, 2019)

- "In the context of paper transactions, California courts have deemed analogous incorporations by reference valid and the incorporated terms binding….
- Federal courts likewise have recognized the general enforceability of similar online agreements that require affirmative user assent. *See, e.g.*, *Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 78–79 (2d Cir. 2017) (applying California law and determining user assented to arbitration provision contained in online Terms of Service where enrollment page clearly stated user's enrollment signaled assent to terms and terms were reasonably conspicuous even though lengthy); *see also* *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014) ("[C]ourts have consistently enforced [terms of use] agreements where the user had actual notice of the agreement. ... [or] where the user is required to affirmatively acknowledge the agreement before proceeding with use of the [service.]")."

Alan Ross Machinery Corporation v. Machinio Corporation 2018 WL 3344364, (N.Ill. July 9, 2018)

- **Whether browsewrap containing terms against web scraping enforceable.**
- "Alan Ross argues that Machinio had constructive knowledge of the terms and conditions because of their conspicuous placement on the website.. (arguing the terms and conditions link was prominently displayed and appeared at the bottom of every webpage). Nevertheless, hyperlinking the terms and conditions at the bottom of every page is insufficient to provide adequate constructive notice to create a contract based on a browsewrap agreement. …
- Without allegations that Machinio had notice of their existence, the terms and conditions are not an enforceable agreement…Alan Ross fails to state a breach of contract claim because it fails to allege an enforceable contract exists."

Hurst Real Estate Service Inc. v. Great Lands Corporation, 2018 ONSC 4824

- "The defendants also submit that s. 23(1) of the Regulations to the *Real Estate and Business Brokers Act*, 2002 (O. Reg. 567/05) requires that a claim for commission cannot be brought unless the agreement upon which the action is brought is in writing and signed by or on behalf of the person who is required to pay the commission."
- "The defendants also submit that the email exchanges confirming Mr. Sadr's offer and Mr. Hurst's acceptance are not valid under the Regulation because they are not signed by either party. The emails do not include an original handwritten signature, which is not possible on email exchanges that are made electronically. However, the respective emails end with a typed version of the sender's name, his title and the name of the corporation he represents. I am satisfied that in this digital age in which commerce is routinely conducted with the assistance of information technology, this type of electronic signature meets the requirement under the Regulation that the offer be "signed by or on behalf of the person required to pay the commission.""

Polygon Metalworks Int'l Inc. v Ellisdon Corporation, 2018 BCSC 1448

- **Was an email notice of contract termination effective?**
- "Article 32 of the subcontract sets out the addresses for notices for the parties. These addresses are defined in the contract as the physical addresses of EllisDon and Polygon. Article 32.02 states that all notices shall be in writing and are deemed to be received by the addressee on the date of delivery. The provision then sets out deemed dates of delivery for notices delivered by hand, registered post, and regular post."
- " I find that the Polygon subcontract did not prohibit delivery of notices by any other means than delivery to the physical addresses of the parties. The subcontract established deemed delivery dates for certain methods of delivery. This does not mean that the parties could not deliver communications by email. The parties communicated by email throughout their relationship and I was provided with no evidence of written communication other than by email. I find that EllisDon's decision to provide notices of default and the notice of termination to Polygon by email was not prohibited by the Polygon subcontract."

Online Remedies/Governance/Jurisdiction

Free and open Internet / Internet Exceptionalism

Rule of Law

Innovation (Impact assessment / algorithm responsibility)

Innovation (move quickly and break things)

Personal Information (commodity)

Personal Information (respect for individual autonomy / privacy by design)

ISPs / OSPs (Immunities / safe harbours, limited liability for automated harms)

ISPs / OSPs (Accountability / responsibility)

Territoriality

Extra-territoriality / sovereignty / internet fragmentation

South Dakota v. Wayfair, Inc., 138 S. Ct. 2080

- **Should the Supreme Court reverse a prior precedent under the Commerce Clause that prohibited a State from collecting sales tax from an online retailer unless the retailer had a physical presence in the State?**
- "The "dramatic technological and social changes" of our "increasingly interconnected economy" mean that buyers are "closer to most major retailers" than ever before— "regardless of how close or far the nearest storefront…Between targeted advertising and instant access to most consumers via any internet-enabled device, "a business may be present in a State in a meaningful way without" that presence "being physical in the traditional sense of the term."… A virtual showroom can show far more inventory, in far more detail, and with greater opportunities for consumer and seller interaction than might be possible for local stores. Yet the continuous and pervasive virtual presence of retailers today is, under *Quill*, simply irrelevant. This Court should not maintain a rule that ignores these substantial virtual connections to the State.""

South Dakota v. Wayfair, Inc., 138 S. Ct. 2080

"Further, the real world implementation of Commerce Clause doctrines now makes it manifest that the physical presence rule as defined by *Quill* must give way to the "far-reaching systemic and structural changes in the economy" and "many other societal dimensions" caused by the Cyber Age. *Direct Marketing*, 575 U.S., at ___, 135 S.Ct., at 1135 (KENNEDY, J., concurring). Though *Quill* was wrong on its own terms when it was decided in 1992, since then the Internet revolution has made its earlier error all the more egregious and harmful."

Paramount Fine Foods and Fakih v Johnston, 2019 ONSC 2910

- **Remedies for online posting false and malicious hate speech videos.**
- "The Court of Appeal has indicated that, where the defamatory statements are disseminated over the Internet, these factors must be examined in light of the ubiquity, universality and utility of that medium. Communication via the internet is instantaneous, seamless, interactive, blunt, borderless and far reaching. As such, "internet defamation is distinguished from its less pervasive cousins, in terms of its potential to damage the reputation of individuals and corporations, by […] its interactive nature, its potential for being taken at face value, and its absolute and immediate worldwide ubiquity and accessibility."
- "As recognized by the Court of Appeal, given the "extraordinary capacity" of the internet to replicate defamatory statements "almost endlessly", "the truth rarely catches up with a lie"."

Paramount Fine Foods and Fakih v Johnston, 2019 ONSC 2910

- "In conclusion, I feel compelled to stress the wider societal issues that this very disturbing case represents. In this fractious 21st century – where social media and the internet now allow some of the darkest forces in our society to achieve attention - these issues are numerous and profound, and their impact extends well beyond the borders of this country."
- "…defendants are ordered to pay $2.5 million in damages...
- …defendants are required to remove and/or destroy any copy of or reference to the videos and the defamatory content identified in this action from any source, medium or place accessible to any third party….
- …defendants are permanently restrained, or anyone acting on their behalf, direction, or in conjunction with them, from… disseminating, posting on the Internet, publishing, or broadcasting in any manner whatsoever, either directly or indirectly, any defamatory statements concerning the plaintiffs or its officers, directors, shareholders, employees or related entities."

Manuel v Economic Freedom Fighters, [2019] ZAGPJHC 157 (30 May 2019)

- "The respondents are ordered to remove the statement, within 24 hours, from all their media platforms, including the first and third respondents' Twitter accounts;
- The respondents are ordered, within 24 hours, to publish a notice on all their media platforms, on which the statement had been published, in which they unconditionally retract and apologise for the allegations made about the applicant in the statement.
- The respondents are interdicted from publishing any statement that says or implies that the applicant is engaged in corruption and nepotism in the selection of the Commissioner of the South African Revenue Service."

Eva Glawischnig-Piesczek v Facebook Ireland Limited
CJEU Case C-18/18 (Opinion Advocate General)

- "The internet's not written in pencil, it's written in ink, says a character in an American film released in 2010. I am referring here, and it is no coincidence, to the film The Social Network.
- In fact, the key issue in the present case is whether a host which operates an online social network platform may be required to delete, with the help of a metaphorical ink eraser, certain content placed online by users of that platform."
- A Facebook user published a disparaging comment about the applicant "accusing her of being a 'lousy traitor of the people', a 'corrupt oaf' and a member of a 'fascist party'."

Eva Glawischnig-Piesczek v Facebook Ireland Limited
CJEU Case C-18/18 (Opinion Advocate General)

- "To conclude, it follows from the foregoing considerations that the court of a Member State may, in theory, adjudicate on the removal worldwide of information disseminated via the internet. However, owing to the differences between, on the one hand, national laws and, on the other, the protection of the private life and personality rights provided for in those laws, and in order to respect the widely recognised fundamental rights, such a court must, rather, adopt an approach of self-limitation. Therefore, in the interest of international comity, to which the Portuguese Government refers, that court should, as far as possible, limit the extraterritorial effects of its junctions concerning harm to private life and personality rights. The implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person. Thus, instead of removing the content, that court might, in an appropriate case, order that access to that information be disabled with the help of geo-blocking."

UTV Software Communications Ltd v 1337X.TO High Court Delhi, 10 April, 2019, CS(Comm) 724/2017

- **Whether an infringer of copyright on the internet is to be treated differently from an infringer in the physical world?**
- "However, many believe that Internet is a unique highway or a separate space (i.e. Cyberspace) to be left totally free i.e. unrestricted. They believe that this space should be left free to be used by an infringer or by a law abiding individual simultaneously. Internet exceptionalists, such as the Electronic Frontier Foundation, are defined by the belief that because the Internet is exceptional, most rules that apply offline should not apply online. Followers of this school of thought believe that the Internet is first and foremost about individual freedom, not about collective responsibility. Their view is that the Internet's chief function is to liberate individuals from control by, or dependence on Government and Corporations. They believe in the maturity of the public. The followers of this school of thought acknowledge that online piracy comes at the cost of legal sales, but they rationalize this loss by saying that it only hurts the profits of content firms, implying that if the choice is between infringement that rewards consumers with free content versus legality that helps corporations, then the former is to be preferred."

UTV Software Communications Ltd v 1337X.TO High Court Delhi, 10 April, 2019, CS(Comm) 724/2017

- "However, this Court finds that the majority of piracy websites are in it not for any ideological reason but for one reason: to make money. Modern digital piracy is a multibillion-dollar international business…
- Also should an infringer of the copyright on the Internet be treated differently from an infringer in the physical world? If the view of the aforesaid Internet exceptionalists school of thought is accepted, then all infringers would shift to the e-world and claim immunity!
- "A world without law is a lawless world. In fact, this Court is of the view that there is no logical reason why a crime in the physical world is not a crime in the digital world especially when the *Copyright Act* does not make any such distinction."

UTV Software Communications Ltd v 1337X.TO High Court Delhi, 10 April, 2019, CS(Comm) 724/2017

- **Whether seeking blocking of a website dedicated to piracy makes one an opponent of a free and open internet?**
- "If the views of Internet exceptionalists were to be accepted, then a boon like Cyberspace would turn into a disaster. Further, just as supporting bans on the import of ivory or cross-border human trafficking does not make one a protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open Internet. Consequently, this Court is of the opinion that advocating limits on accessing illegal content online does not violate open Internet principles.
- The key issue about Internet freedom, therefore, is not whether the Internet is and should be completely free or whether Governments should have unlimited censorship authority, but rather where the appropriate lines should be drawn, how they are drawn and how they are implemented."

Blocking orders

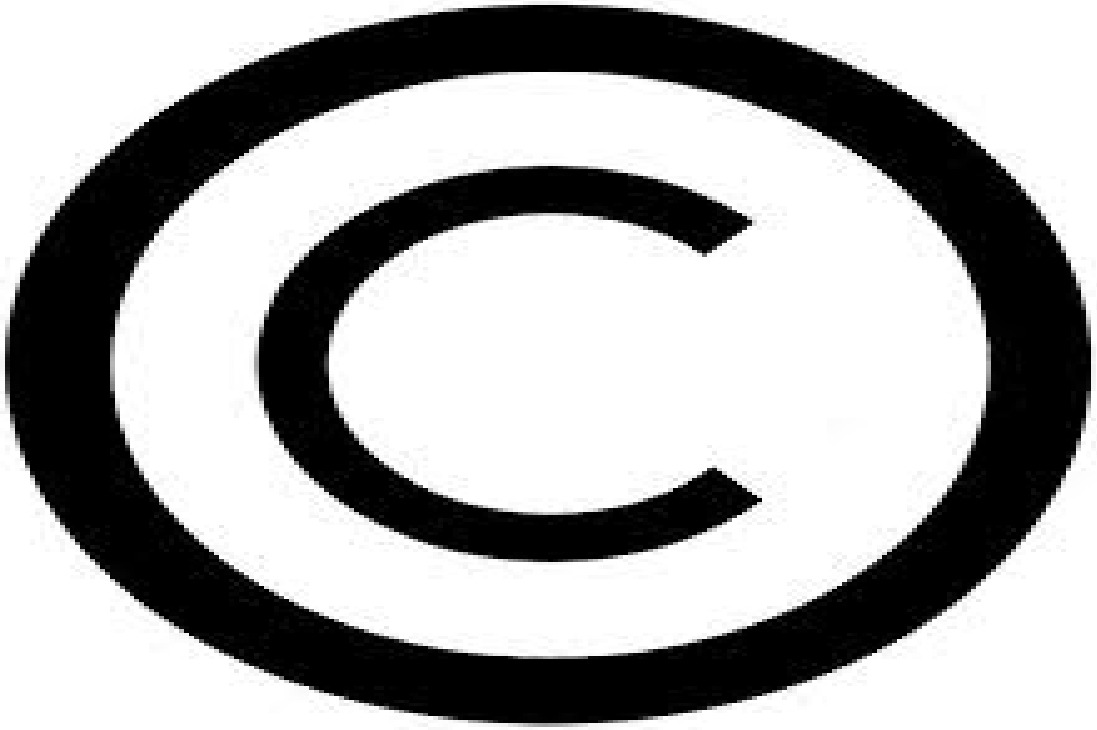
- Television Broadcasts Limited v Telstra Corporation Limited [2018] FCA 1434 (sites streaming to Internet Streaming devices (ISDs))
- Roadshow Films Pty LTD v Telstra Corporation Limited Aust. F.C. 20 December, 2018 (181 domains linked to 78 sites)
- Australasian Performing Right Association Ltd v Telstra Corporation Limited [2019] FCA 751 (stream ripping sites)
- S.A.S Elsevier et al v S.A. Orange Tribunal De Grande Instance de Paris 29 Nov., 2018 (Sci-Hub)
- UTV Software Communications Ltd v 1337X.TO High Court Delhi, 10 April, 2019, CS(Comm) 724/2017 (multiple “rogue” sites including BitTorrent sites)

FairPlay Coalition – Application to disable online access to piracy websites, Telecom Decision CRTC 2018-384

- "Section 36 of the *Telecommunications Act* limits the ability of carriers to control the content of messages carried over their networks without prior Commission authorization. While this section gives the Commission the explicit power to authorize an ISP to block a website, the proposed regime would go further and require such blocking pursuant to a Commission order. Because section 36 confers an authorizing power and not a mandatory power, the power to mandate blocking must be found elsewhere and must relate to subject matter that is clearly within the Commission's jurisdiction under the *Telecommunications Act*."
- …the Commission determines that it does not have the jurisdiction under the *Telecommunications Act* to implement the proposed regime and, consequently, it will not consider the merits of implementing the regime. The Commission therefore denies the FairPlay Coalition's application."

Statutory Review of the Copyright Act, Report of the INDU Committee

- "The Committee…agrees that there is value in clarifying within the Act that rights-holders can seek injunctions to deny services to persons demonstrably and egregiously engaged in online piracy, provided there are appropriate procedural checks in place. The Committee also supports amending the *Telecommunications Act* to remove any procedural duplication or unnecessary hurdles.
- The Committee does not, however, support the development of an administrative regime to these ends. It is for the courts to adjudicate whether a given use constitutes copyright infringement and to issue orders in consequence. The courts already have the expertise necessary to protect the interests of all involved parties."



Collett v. Northland Art Company Canada Inc., 2018 FC 269

- **Does framing infringe copyright?**

  - "The evidence that Mr. Collett's website had been linked to the Northland site is uncontroverted, as is the evidence that the link was neither removed nor disabled until 2015. The evidence of the Tamburi brothers on this issue was confused, evasive and in many respects incredible. I am satisfied on a balance of probabilities that Northland continued to maintain a link to Mr. Collett's website knowing it was not authorized to do so. In doing so Northland infringed Mr. Collett's copyright in the "Website Home Page" which included a reproduction of the image "Winter Blues" and the "Bio Page"."

Toronto Real Estate Board v Mongohouse.com, Federal Court Order, April 15, 2019, File T-1653-18

- **Does website scraping infringe copyright?**
- "It is hereby ordered and declared that the unauthorized copying, data scraping, downloading, display, distribution, access to make available for distribution, streaming for public display any TREB MLS® data is a breach of TREB's proprietary rights and copyrights associated with the TREB MLS®.
- It is hereby ordered and declared that any access to the TREB MLS® other than as authorized by TREB using any means to avoid, bypass, deactivate, impair, or to circumvent in any manner a technological protection measure ("TPMs") is a breach of Section 41 of the Act and is an infringement of TREB's rights."
- Injunctive relief ordered.

Thomson v. Afterlife Network Inc., 2019 FC 545

- **Class remedies against operator of website publishing >1.1.4 million obituaries for moral rights and copyright infringement.**
- "An injunction is a normal remedy for copyright infringement, in accordance with section 34 of the Copyright Act. An injunction is warranted to stop Afterlife from continuing to infringe the Class Members' rights in the original works. Afterlife refused some families' requests to remove obituaries and did not take the website down until this Application was filed. I agree that the injunction should also name Mr. Leclerc, who is the director of Afterlife and has continued to post obituaries at his new website, Everhere."
- "Aggregate damages on a class wide basis are appropriate and are awarded in the amount of $20,000,000, representing: statutory damages in the amount of $10,000,000; and aggravated damages in the amount of $10,000,000."

Rogers Communications Inc. v. Voltage Pictures, LLC, [2018] 2 SCR 643

"An ISP can recover its costs of compliance with a *Norwich* order, but it is not entitled to be compensated for every cost that it incurs in complying with such an order. Recoverable costs must be reasonable and must arise from compliance with the Norwich order. Where costs should have been borne by an ISP in performing its statutory obligations under the notice and notice regime, these costs cannot be characterized as either reasonable or as arising from compliance with a *Norwich* order, and cannot be recovered."

Rogers Communications Inc. v. Voltage Pictures, LLC, [2018] 2 SCR 643

- "Similarly, the notice and notice regime has not displaced the copyright owner's burden, at common law, of bearing the ISP's reasonable costs of compliance with the *Norwich* order. However, the statutory regime prohibits an ISP from charging a fee for performing any of its obligations arising under the regime. Accordingly, an ISP should not be permitted to recover the cost of carrying out any of the obligations, express or implicit, that will have arisen under the regime, even if it carries out the obligations only after having been served with a *Norwich* order. Otherwise, the distribution of financial burden which Parliament decided upon would be undermined by imposing upon copyright owners an obligation which was specifically allocated to ISPs in the notice and notice regime."
- On the evidence needed to obtain a *Norwich* order in a file sharing case, see, ME2 Productions, Inc. v. Doe, 2019 FC 214.

Keatley Surveying Ltd. v. Teranet Inc., Supreme Court Docket 37863

- "Intellectual property - Copyright, Infringement, Legislation, Interpretation - Intellectual property - Copyright - Crown copyright - Infringement - Legislation - Interpretation - Class action for breach of copyright by surveyors whose land surveys were scanned and copied into an online digital database - Does section 12 of the Copyright Act, R.S.C. 1985, c. C-42, transfer copyright in plans of survey that are filed in provincial land registry offices from the surveyor creators to the government."
- See also, P.S. Knight Co. Ltd. v. Canadian Standards Association, 2018 FCA 222, leave to SCC dismissed (Crown prerogative does not transfer copyright in CSA Codes to Crown where document is only incorporated by reference in statutes).


AWARDED
TOP 50
COPYRIGHT
BLOG

VANCOUVER

Suite 1300, 777 Dunsmuir Street
P.O. Box 10424, Pacific Centre
Vancouver BC V7Y 1K2
Tel: 604-643-7100
Fax: 604-643-7900
Toll-Free: 1-877-244-7711

CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500
Fax: 403-260-3501
Toll-Free: 1-877-244-7711

TORONTO

Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto (Ontario) M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673
Toll-Free: 1-877-244-7711

MONTRÉAL

Suite 2500
1000 De La Gauchetière Street West
Montréal QC H3B 0A2
Tel: 514-397-4100
Fax: 514-875-6246
Toll-Free: 1-877-244-7711

QUÉBEC

Le Complexe St-Amable
1150, rue de Claire-Fontaine, 7e étage
Québec QC G1R 5G4
Tel: 418-521-3000
Fax: 418-521-3099
Toll-Free: 1-877-244-7711

UNITED KINGDOM & EUROPE

125 Old Broad Street, 26th Floor
London EC2N 1AR
UNITED KINGDOM
Tel: +44 (0)20 7786 5700
Fax: +44 (0)20 7786 5702

mccarthy tétrault