Dealing with Digital Property in Civil Litigation

Jeremy de Beer
Tracey Doyle, Belmore Neidrauer LLP
Dealing with Digital Property in Civil Litigation

JEREMY DE BEER AND TRACEY DOYLE*

I. INTRODUCTION

For roughly two decades, a set of difficult questions has been creeping up on the civil litigation system. How should lawyers, judges and other stakeholders strategically address cases arising from cyberspace? Do digital technologies, especially information communication technologies like the Internet, fundamentally disrupt our conventional legal frameworks for dispute resolution? Or can we use standard legal rules and concepts to resolve controversies triggered by new technological phenomena? Which is the doctrinally preferable approach? Is there an overarching theory offering insights into the matter, or does the nature of the problem defy any universal solution?

This article aims to shed light on the conceptual, doctrinal and practical issues regarding digital property law by weaving together several facets of the subject. Legislative schemes for the digital environment have emerged to cover some issues but not others. The debate about further statutory reform to deal with digital property is ongoing. Litigated cases in Canada are becoming increasingly common, and those that arise tend to be complex and significant. With this article, we facilitate better understanding of digital property issues among the bench and the bar, and offer a principled approach to legal policymakers grappling with law reform in this context. The approach we put forward is one based on technological neutrality, in the substantive functional sense not the minimalist notion of media neutrality.

We begin by providing important historical perspective on the debate about digital property rights, tracing its evolution over the past 20 years. We then canvass six distinct areas of law where digital property issues are engaged:

- the legal definition of digital assets as property;
- the protection of digital property against damage;
- dealing with digital property in life and on death;

* Jeremy de Beer is a Full Professor at the Faculty of Law, University of Ottawa. This article is derived in part from an earlier paper prepared for the National Judicial Institute. Funding to support this work was provided by the Social Sciences and Humanities Research Council (SSHRC). Tracey Doyle is a Student-at-Law at Borden Ladner Gervais LLP. The opinions expressed herein do not necessarily reflect the opinions of the firm or its clients.
digital property and privacy rights;
jurisdiction over cyberspace; and
the technological regulation of digital property.

After discussing the most significant legal developments during the past two
decades, we conclude with strategic insights for judges, practitioners and others
faced with digital property issues in the future. We show how substantive
technological neutrality can serve as a guiding principle connecting each of the
digital property doctrines we review.

1. The Law of the Horse?

In the 1990s cyberspace was a burgeoning concept changing society. Through
cyberspace, and the Internet in particular, the public had unprecedented access
to the world’s information resources. This access gave rise to a host of legal
concerns, amongst which was whether fundamental principles of property, tort,
contract and related fields of law could be easily applied in a new, digital
domain.

Many legal scholars and practitioners recognized the unique nature of
cyberspace and discussed how these issues could be best addressed. One
especially noteworthy discussion took place during a conference in 1996 at the
University of Chicago. There, Judge Frank Easterbrook of the United States
Court of Appeals for the 7th Circuit spoke about the law of cyberspace.
Surprisingly, Judge Easterbrook did not speak about how society should make
unique laws aimed at regulating cyberspace. Instead, his position was that there
is no need for cyberlaw. He famously analogized cyberlaw to “the law of the
horse” and argued that just as the principles of contract, tort and property law
can be applied to regulate horses, so too can they be applied to any legal issue
arising out of cyberspace.1

Easterbrook’s comments challenged cyberlaw scholars and practitioners to
think carefully about their field. Lawrence Lessig reacted by rebutting
Easterbrook’s proposition with an article in the Harvard Law Review.2 In it,
Lessig systematically described the fundamental differences between “cyber
space” and “real space” and argued that the nature of these differences
necessitated a new legal approach.3 Lessig pointed to issues such as age
verification for access to online pornography, privacy issues that could arise out
of hacking databases and the challenges of dealing with intellectual property
online as illustrative issues requiring distinct cyber-solutions.4

of Chicago Legal Forum 207.
3 Ibid at 506-510.
4 Ibid at 518.
Easterbrook and Lessig’s debate has since become required introductory reading for students of law and technology, painting the backdrop for the development of cyberlaw.\(^5\) Google Scholar counts almost 1100 combined citations to the articles. These and related works have framed our thinking about such questions as: Is cyberspace a place?\(^6\) What are the laws of virtual worlds?\(^7\) How do digital technologies change theories of free speech?\(^8\) Which schemes best protect privacy and democracy online?\(^9\) With extensive work on topics from all those just mentioned to cybercrime to online contracts, few legal fields have escaped analysis through this lens.

Roughly 20 years after Easterbrook and Lessig exchanged views, lawmakers across Canada have not yet developed a thoroughly tailored approach to deal with digital property. Does that mean Easterbrook was right? That general principles work fine to solve digital disputes? Perhaps not, since in some areas specific codes have emerged to address digital property rights. In the following sections of this article, we explore a range of digital property-related issues to assess how they are governed by standard legal principles and/or \textit{sui generis} cyberlaws.

2. The Principle of Technological Neutrality

The debate between Easterbrook and Lessig about cyberlaw can also be seen as a proxy for deeper questions about the basic principle of technological neutrality. Lately, technological neutrality has garnered the most attention from the Supreme Court of Canada in the realm of copyright in digital works. The concept is, however, more fundamental to cyberlaw than the Court’s recent copyright jurisprudence would suggest.

In the context of copyright, the Supreme Court’s approach to technological neutrality is aptly demonstrated in a series of cases decided since the turn of the century. For those seeking a comprehensive analysis of the principle’s history and application in copyright cases, excellent work has been done recently by Canadian law professors including Craig, Hagen and Hutchinson.\(^10\) In this

---


\(^10\) Carys Craig, “Technological Neutrality: (Pre)Serving the Purposes of Copyright Law” in Michael Geist, ed, The Copyright Pentalogy: How The Supreme Court of Canada Shook the Foundation of Copyright Law (Ottawa: University of Ottawa Press, 2013);
section, we highlight key points to demonstrate the principle’s relevance to the field of cyberlaw generally, and more specifically digital property disputes.

In SOCAN v CAIP, the Supreme Court interpreted the Copyright Act to promote Internet communications by exempting from liability service providers’ activities that are “reasonably useful and proper to achieve the benefits of enhanced economy and efficiency.”11 While the Court did not discuss the principle of technological neutrality, its purposive approach of generously interpreting a safe harbour provision for Internet intermediaries had the practical effect of encouraging service providers to adopt more technologically advanced practices, such as caching.

Robertson v Thomson Corp raised the question whether the Globe and Mail could reproduce articles contributed by freelancers for the print edition of its newspapers in electronic databases.12 According to the majority, they cannot, partly because of the principle of media neutrality. “Media neutrality,” wrote the majority, “means that the Copyright Act should continue to apply in different media, including more technologically advanced ones.”13 Justice Abella, writing for four dissenting judges, had a more nuanced view of neutrality. She wrote that the reproduction of articles in a database is the electronic analogy to stacking print editions of a newspaper on a shelf, suggesting that substance is more important than form.14

A trio of cases in 2012, part of the “copyright pentalogy”15 consisting of five interrelated decisions released by the Supreme Court on the same day, also address technological neutrality in online transactions.16 ESA v SOCAN, Rogers

---

13 Ibid at para 49 per LeBel and Fish JJ.
14 Ibid at paras 72-79, 85-91, 93, 98 per Abella J (dissenting).
In ESA, the issue was whether streaming video games containing music via the Internet triggered liability for both reproduction royalties and communication royalties — separate and distinct rights split up by authors for administration by two different collecting societies. Justices Abella and Moldaver relied on technological neutrality, in a substantive and functional sense, in their majority judgment: “In our view, there is no practical difference between buying a durable copy of the work in a store, receiving a copy in the mail, or downloading an identical copy using the Internet. The Internet is simply a technological taxi that delivers a durable copy of the same work to the end user.”17 To impose extra royalties based solely on the method of delivery would “effectively impose a gratuitous cost for the use of more efficient, Internet-based technologies.”18

The Rogers case was more straightforward, raising the issue whether streaming music online to individuals on-demand constitutes a telecommunication to the public. The Supreme Court held unanimously that it does. The Court cited the formalistic view of media neutrality articulated in Robertson, but in effect applied the principle as one focused on effects. “Whether a business chooses to convey copyright protected content in a traditional, “broadcasting” type fashion, or opts for newer approaches based on consumer choice and convenience, the end result is the same.”19

In SOCAN v Bell, the Supreme Court unanimously held that previews of music offered through Apple’s iTunes online music store were fair dealing for the purpose of consumer research. Technological neutrality was relevant in recognizing users’ rights. The Court declined to consider the aggregate amount of music previewed online, because if “large-scale organized dealings are inherently unfair, most of what online service providers do with musical works would be treated as copyright infringement.”20

The most recent copyright case on technological neutrality is CBC v SODRAC.21 A majority of the Supreme Court held that reproduction royalties are payable by broadcasters who make “broadcast-incidental” copies of music embedded in programming. In this particular case, reference to the

---

principle of technological neutrality was unnecessary given what the majority considered was a clear statutory provision: “though the principles of balancing user and right-holder interests and of technological neutrality are central to Canadian copyright law, they cannot change the express terms of the Copyright Act.”

However, the Court went further than confirming the centrality of technological neutrality to the Act’s interpretation. Also, “the principle of technological neutrality applies to valuation of a reproduction licence, just as it does in determining whether an activity implicates copyright at all.”

“Interpretation and application of the Act are both important in seeking this objective [of technological neutrality].”

Justice Abella, writing in dissent for herself and Justice Karakatsanis on this issue, would have applied the technology neutral principle of functional equivalence to hold that no reproduction royalties at all were payable in this case, while the majority applied the principle at the valuation stage to suggest that the technological context here would “imply relatively low licence fees”.

Craig provides an extremely useful framework to understand what courts have done with technological neutrality in copyright cases. The “restrictive” application is formalistic, merely ensuring that rights continue to apply regardless of the technology involved. An “intermediate” approach is more result-oriented, ensuring the law has consistent effects across different technologies. An “expansive” understanding of technological neutrality is purposive, aiming for substantive non-discrimination between functional equivalents.

The principle of technological neutrality is not limited to copyright law, of course. It can be applied to any area of law which may be affected by the evolution of technology. For example, technological neutrality was a foundational concept in the development of e-commerce laws, such as the Uniform Electronic Commerce Act, which removes barriers to e-commerce by making the law media neutral. The effect of this type of legislation is to ensure that contracts remain binding regardless of whether they are agreed to on paper, in an email, or through an automated voice attendant.

--

22 Ibid at para 51.
23 Ibid at para 67.
24 Ibid at para 68.
25 Ibid at para 179.
26 Ibid at para 75.
Gregory explains technological neutrality in the UECA and its inspiration the UN Model Law: “they do not simply define writing as including an electronic record, or define signature as including an electronic signature. This was thought too rigid an approach that risked including too many electronic records or allowing electronics in too many situations. Rather, the law seeks to isolate the essential policy functions of the requirement and state how those functions can be achieved electronically.”

When explaining particular applications of the UECA, such as signatures, Gregory continues: “In all its functional equivalence rules, the Uniform Act does not intend to change the substance of the existing law. It intends only to make the law media neutral, equally applicable to paper and to electronic documents.”

It is interesting, in hindsight, to compare this explanation of one of cyberlaw’s earliest legislative frameworks with Professor Craig’s more recent framework and the Supreme Court’s (especially Justice Abella’s) latest rulings differentiating media neutrality and functional equivalence.

The difference between formal media neutrality and functional substantive equivalence has also been highlighted in Kerr’s prescient work on artificial intelligence and online contracting: “it is important not to confuse the principle of technological neutrality with the mistaken idea that technologies are themselves neutral” he writes. The more interesting question Kerr raises is “what should our policy objectives be in cases where the technologies are themselves not neutral as between the creators and the users of the relevant technologies?”

Whether in copyright, e-commerce, artificial intelligence or digital property issues, technological neutrality can — if employed robustly — establish a functional rather than formal equivalence between real space and in cyberspace. This equivalence is particularly important when legal issues arising out of technological advancements are not adequately addressed by statutory provisions. A minimalist application of technological neutrality, just
to fill legislative gaps, would basically mirror Easterbrook’s argument that general principles of property law should be applied to legal issues in cyberspace. However, in order to achieve functional equivalence, courts must ensure that the law will have the same effect in cyberspace as it does in real space. In these circumstances, “to achieve the perceived benefits of technology neutrality, lawmakers must properly discriminate among different technologies”, explains Greenberg.36 Craig notes that the principle of technological neutrality “cannot perform this role effectively if conceived (or rhetorically invoked) as a limited principle of formal non-discrimination”37 This, essentially, is Lessig’s point too. Cyberlaw is not the law of the horse. One cannot merely apply the same standard rules of contracts, tort, property or other areas of law to issues in a radically different digital environment. In the following section of this article, we consider various digital property-related doctrines to further unpack that insight.

II. CURRENT ISSUES IN DIGITAL PROPERTY LAW

1. Defining Digital Assets as Property

One of the most fundamental questions that arises in considering cyber-property issues is: Are digital assets “property”? In Canada, the issue arose in Tucows.Com Co. v Lojas Renner S.A.38 Tucows was a Canadian wholesaler of domain names. It purchased the domain name <www.renner.com>, along with 30,000 other domain names, intending to resell it. When a company registers or acquires a domain name, they agree to a uniform dispute resolution policy (known as the UDRP) through which disagreements will be settled. Renner is a department store operator in Brazil and owner of the trademark “Renner”. Attempting to acquire control over the renner.com domain, the Brazilian company started proceedings under the UDRP. Rather than responding to these proceedings, Tucows filed a statement of claim in an Ontario court seeking a peremptory declaration that it had the rights to the domain name.

A procedural issue arose when Tucows filed this statement of claim outside of Ontario, without leave of the Court. Under Ontario’s Rules of Civil Procedure39

---

a party can only file a statement of claim outside of Ontario without leave when
the claim pertains to personal property in Ontario. The Court faced a
fundamental definitional problem: Is a domain name property, and if so, is it
personal property, and if so, where is it located? Paragraphs 41-72 of Justice
Weiler’s decision address those issues.

She begins her reasons on this issue with apparently unintentional
metaphorical references to cyberspace as a place. She writes, for example, that
the role of a domain name is to provide “an address for computers” and allow
consumers to “navigate the Internet”.40 Then, her review of international cases
and academic commentary revealed a growing consensus that domain names are
property. She found that view aligns with leading property theorists’ and
scholars’ understanding of “property” as a malleable bundle of rights, the core
attribute of which is exclusivity, not tangibility. It is, she held, also consistent
with Justice Binnie’s decision of the Supreme Court of Canada that a fishing
license can be property for the purpose of bankruptcy and insolvency
proceedings.41 Its intangibility is irrelevant.

Justice Weiler’s decision provides an excellent overview of what constitutes
digital property. Moreover, she held that the property is located in Ontario,
given the location of the registrant and its computer servers. In this respect, her
decision addresses the increasingly common and thorny issue of jurisdiction in
cyberspace, which is raised below as one of the crucial areas for further legal
development.

Domain names are not the only context where the fundamental nature of
digital property is questioned. Issues have also arisen over digital real estate in
virtual worlds. For example, several cases have been brought against the
creators of the game “Second Life”.42 As a part of this game, players can buy
and sell virtual items for real world cash. Civil litigation has focussed mainly on
allegations of virtual “expropriation” of the plaintiffs’ digital property, plead on
a combination of copyright, contract and other doctrinal grounds. Although
these cases, a mix of individual and class actions, settled, they illustrate both the
value of digital assets and how preventing one from being able to designate
ownership of these assets may substantially impact this value.

Other cases have raised questions about whether social media accounts can be
property, and if so, who owns them. For example, PhoneDog v Kravitz,43 is a

40 Tucows.Com Co. v Lojas Renner SA, 2011 ONCA 548 at para 44, leave to appeal refused
2012 CarswellOnt 6413 (SCC).
41 Saulnier (Receiver of) v Saulnier, [2008] 3 SCR 166.
42 Bragg v Linden Research Inc, 487 F Supp 2d 593 (ED Pa, 2007); Evans v Linden Research
Inc, CV No 10-1679 (ED Pa, February 3, 2011); Evans v Linden Research Inc, No C-11-
01078 (ND Cal, October 25, 2013); FireSabre Consulting LLC v Linden Research Inc, No
11-CV-4719 (SDNY, September 26, 2013).
43 PhoneDog v Kravitz, No C 11-03474 MEJ (ND Cal).
recently settled case where a California court had allowed a company’s claim for conversion of digital property to proceed, on the basis that a former employee retained and used a Twitter account after the employment relationship had terminated. Similar cases have arisen regarding not just Twitter but also Facebook profiles, Google groups, and LinkedIn accounts. The common threads in these so-far mostly American cases are usually allegations of interference with economic relations, and theft of trade secrets, highlighting the intersection between tangible, digital and intellectual property issues. Judges and counsel can most easily resolve these cases by conceptually separating the account itself from the information it contains, such as customer contacts or potentially goodwill. Parties could generally avoid disputes altogether by agreeing on ownership in advance.

2. Protecting Digital Property from Damage

Property rights do not enforce themselves. While a declaration may be useful validation, in practice property owners must rely on criminal or civil laws to obtain remedies for infringement. Criminal laws prohibit wrongs including theft and criminal trespass. In the civil context, property rights are protected by actions in tort, such as conversion and also trespass. In cyberspace, a question arises as to which sort of trespass might apply. If cyberspace is really a place, then perhaps trespass to land is the appropriate action for interference with virtual real estate. However, choosing pragmatism over metaphor means bringing a case instead for the lesser-used tort of trespass to chattels. The tort of trespass to chattels is known as “little brother” of conversion, because it permits claims for minor interferences with personal property, which fall short of fully depriving the rightful owner or possessor of her own rights. It is this tort which has morphed into the doctrine of cyber-trespass.

Thrifty-Tel Inc v Bezenek was one of the first instances where a court considered trespass to chattels in the context of computer systems. Here, children used phone signals to hack long distance telephone services without paying for them. The Court noted that the signals generated by the children overburdened the phone system and this was sufficient harm to justify the trespass to chattels claim. The finding in Thrifty-Tel was later followed in

44 See, for example, Maremont v Susan Fredman Design Group, 2011 LEXIS 26441 (ND III, March 15, 2011).
45 See, for example, Kremer v Tea Party Patriots Inc, 2012 WL 639134 (Ga App Ct, February 29, 2012).
46 See, for example, Eagle v Morgan, 2012 WL 4739436 (ED PA, October 4, 2012).
47 Criminal Code, RSC 1985, c C-46 ss 177, 328.
49 Thrifty-Tel Inc v Bezenek, 54 Cal Rptr 2d 468 (Cal Ct App, 1996).
CompuServe Inc v Cyber Promotions Inc,\textsuperscript{50} which dealt with unsolicited bulk email ("spam") that was sent to user addresses on the CompuServe network. The plaintiff alleged that these emails prompted its users to unsubscribe to the server. The Court ultimately found that the bulk emails occupied network memory, resulted in loss of users and consumed employee time. Since trespass to chattels only required the plaintiff to show the defendant interfered in a way so that the value of the chattel was impaired, the Court found that the requisite harm was met and the claim was successful.

After \textit{Thrifty-Tel} and \textit{CompuServe} laid the ground work for cyber-trespass, the California Supreme Court decided the seminal case, \textit{Intel v Hamidi}.\textsuperscript{51} A majority of that Court found that a former Intel employee did not commit the tort of trespass to chattels when he used Intel’s computer system to send six unsolicited emails over a two-year period to thousands of Intel’s current employees. The Court surveyed other cases involving robotic data collection, i.e. “bots” that visit websites very frequently to compare prices, auto-dialing through telephone systems, and large-scale spamming operations. The Court distinguished cases such as \textit{Thrifty-Tel} or \textit{CompuServe} because in those instances there was proof of some actual or threatened harm to the computer system. Intel could not show any such harm and therefore the claim for cyber-trespass was unsuccessful.

There were two dissenting opinions in the case, which put forward broader interpretations of property law that would have found some harm to Intel justifying their cause of action against Hamidi. Judge Brown analogized the defendant’s actions to spray painting an unwanted message on a citizen’s private property. He argued that the damage is not merely in the time it takes to remove the message, but also in the content of the message itself. Judge Mosk furthered this proposition and argued that trespass to chattels has never been limited to physical damage.

Academic commentary and theoretical perspectives on property law were instrumental in all of the judges’ opinions. The Court considered work from scholars such as Richard Epstein, who supports the position that an Internet server cannot be analogized to chattels because it is not moveable; rather, a website is more like real property. Additionally Epstein argues that when a server’s website is slowed down this can be a significant harm to its consumer base, which is not often considered in real space.\textsuperscript{52} Other scholars take the position that broadening the scope of cyber-trespass could result in the Internet community having to ask permission before visiting websites or even sending emails.\textsuperscript{53} Arguments on both sides advocated for a kind of Internet

\textsuperscript{50} \textit{CompuServe Inc v Cyber Promotions Inc}, 962 F Supp 1015 (SD Ohio, 1997).
\textsuperscript{53} Shyamkrishna Balganesh, “Common Law Property Metaphors on the Internet: The
exceptionalism, with some suggesting cyberspace warrants greater protection for property rights and others suggesting the opposite. Ultimately, the decision boiled down to whether recognizing property rights in cyberspace would facilitate market transactions through licensing, or would instead proliferate technological gridlock by requiring permission merely to visit another person’s website. The California Supreme Court took the more cautious approach and held that six unwarranted emails did not cause sufficient harm for the action to be successful. If reforms are warranted, the Court suggested this was a job for legislators.

The Intel case is a touchstone for legal and policy arguments about why cyber-property rights should or should not be recognized, and how civil law actions to remedy breaches of property rights apply online. In Canada, Century 21 Canada Ltd. Partnership v Rogers Communications Inc involved similar issues to Intel v Hamidi, as well as copyright and contract issues in cyberspace. Century 21 operated a real estate listing website. Zoocasa, a subsidiary of Rogers Communications, operated a website that indexes listings from several other websites, including property descriptions and photographs from the Century 21 website. Century 21 alleged that action violated its contractual terms of use, constituted copyright infringement and was a trespass to chattels. Century 21 substantiated the trespass claims by arguing that after it had sent a cease and desist letter, Zoocasa still accessed the servers on which the Century 21 website was hosted. Zoocasa attempted to defend the claim by arguing that the tort of trespass does not apply to merely accessing computer systems.

The Supreme Court of British Columbia ruled that Zoocasa was liable for breach of contract and copyright infringement. The Court upheld Century 21’s “browse wrap” agreement, i.e. a contractual agreement to be bound by terms of use, formed merely by browsing a website. The Court also found Zoocasa liable for copyright infringement. Most relevant to the topic of this article, Century 21’s claim for cyber-trespass to chattels could not succeed, because the law requires a physical interference with goods. Any interference there might have been (such as in the American cases) was with the computer servers on which Century 21’s website was hosted. In other words, the trespass was not to

---

54 Some cases involve criminal law, rather than civil law, measures to protect digital property. In United States v Aleynikov, 676 F 3d 71 (2d Cir, 2012), the United States Second Circuit Court of Appeals acquitted a former Goldman Sachs employee of “stealing” proprietary code from the bank’s high-frequency trading platform. The Court held the code was not a physical object capable of being stolen under the National Stolen Property Act. The interesting, open question is whether Goldman Sachs might succeed with a civil action for conversion, or more likely, theft of trade secrets.

Century 21’s chattels but to those of its web services provider. Because the owner of those servers was not a plaintiff in the case, the cyber-trespass claim failed (although the contract and copyright claims succeeded). Regrettably, the Court missed the opportunity to reject the basic premise of cyber-trespass, that merely using someone else’s website might constitute trespass to chattels analogous to using someone’s tangible property.

The fundamental question in cyber-trespass cases is whether courts can apply property law grounded in real space to cyberspace. On Easterbrook’s view of cyberlaw, a standard application of trespass to chattels might be warranted. Trespass to chattels requires proof of harm, so courts considering cyber-trespass claims would ask two questions. The first requires identifying the specific “cyber” chattels being assessed. As demonstrated in the case law, chattels in cyberspace could include an email account, a website or the physical computer server that hosts the network. Once the chattels are identified, courts would then assess the harm which occurred as a result of the trespass. This harm is largely dependent upon the nature of the chattel being considered. If it is an email account, then how many emails are enough to cause the owner of the account harm? Did the trespass cause a website to crash? If so, for how long? These questions are evidence that the very nature of trespass in cyberspace is different than trespass in the real world.

An unquestioning application of standard property doctrine to cyberspace is silly in these circumstances. As Goldman points out, the theory and doctrine of cyber-trespass have become dysfunctional. A new approach is warranted: “Given that chattel owners can easily restrict how their Internet-connected chattel is used, they should bear the onus to take the contractual or technological steps to do so. Otherwise, society incurs significant transaction costs for individual users trying to determine their rights to interact with Internet-connected chattel, and overly protective legal doctrines create border cases where users engaged in socially beneficial conduct nevertheless unintentionally commit legal violations.” An example is when someone inadvertently uses someone else’s Internet connection.

The difference between the nature of two spaces necessitates a functionally not formalistically neutral approach.

3. Digital Property Transactions in Life and on Death

Applying general property law principles to digital property should mean that one can designate one’s digital property to another person by way of sale, gift or bequest. Would a functional approach toward technological neutrality suggest otherwise? The question is best answered by distinguishing inter vivos and testamentary transfers, since each raises distinct considerations.

---

56 Ibid at para 299.
(a) *Inter vivos* transfers

In 2009, Amazon and its subsidiary, Kindle, were widely criticized for interfering with their customers' digital property, specifically e-books. Amazon had sold digital copies of George Orwell's *Animal Farm* for use on Kindle electronic reading devices. Amazon later became aware that it lacked the proper copyright authorization to make these sales. To remedy the situation, Amazon wirelessly deleted the book off of thousands of Kindle devices without notice to its users.\(^\text{58}\) Kindle avoided litigation over the matter because its terms of service permitted the drastic action. But what might have happened if the matter weren't addressed by contract? Do you own "your" digital content? If so, what can you do with it?

The doctrinal issue at the heart of this practical problem is known as "exhaustion", which is the law that governs the intersection between tangible and intellectual property rights.\(^\text{59}\) The doctrine, which is rooted in common law, entails that a copyright owner's exclusive right of distribution is exhausted upon the first sale of a physical copy of that item. Digital technologies have significantly complicated this concept.\(^\text{60}\) The idea of re-selling lawfully acquired digital property was squarely addressed by a U.S. District Court in New York in *Capitol Records v ReDigi*.\(^\text{61}\) ReDigi was a virtual second-hand record shop purchasing "used" digital music files from customers and reselling them at a discounted price. ReDigi lost the case because the nature of online file transfers requires reproduction of those files, which is copyright infringement. However, would the Court have found otherwise if ReDigi could resell the media without reproducing the files?

*Oracle v UsedSoft*,\(^\text{62}\) a decision by the Court of Justice for the European Union (CJEU) suggests this is possible. Oracle develops and markets computer software. Upon sale of licenses, users agreed to Oracle's terms of service that stated the license was for perpetual use of the software but was non-transferrable. Despite the user agreement, UsedSoft acquired "used" software licenses from Oracle customers and resold these at a discounted price. The Court of Justice found in UsedSoft's favour by applying the doctrine of exhaustion. This decision was largely influenced by the 2009 European Union's Computer


60 Aaron Perzanowski and Jason Schultz, "Digital Exhaustion" (2011) UCLA Law Review 889 at 929.


62 *UsedSoft GmbH v Oracle International Corp* (C-128/11), [2012] 3 CMLR 44 (Grand Cham).
Program Directive which states that the exhaustion doctrine applies to distribution of software.\textsuperscript{63} But should this reasoning also extend to other forms of digital or intangible property? The European Union’s Copyright Harmonization Directive\textsuperscript{64} suggests that different rules may apply to other forms of digital property because here the directive excludes intangible properties from exhaustion.\textsuperscript{65}

The law on the interface between digital and tangible property in Canada is unsettled. However, the CJEU \textit{Oracle} decision echoes the Supreme Court of Canada’s ruling in \textit{Galerie d’art du Petit Champlain inc v Théberge} which stated “Once an authorized copy of a work is sold to a member of the public, it is generally for the purchaser, not the author, to determine what happens to it.”\textsuperscript{66} However, does this same principle apply to digital works? As was discussed in \textit{ReDigi}, the main issue with resale of digital property is that the process of transfer almost always requires copying. Should the reproduction right in copyright be interpreted to facilitate the growth of markets for second-hand e-books, music or movies? If we understand technological neutrality as functional equivalence, as Justice Abella has so astutely described, and take seriously the Supreme Court’s jurisprudence in cases such as \textit{SOCAN v CAIP} and \textit{ESA v SOCAN}, that law should promote technological efficiency and innovation, the answer seems clear: digital exhaustion does exist in Canadian law.

This view aligns with other leading scholars who argue that courts should invoke the principle of technological neutrality and ignore the copying necessary to transfer digital property,\textsuperscript{67} or focus on the proprietary nature, not physical embodiment, of the digital goods consumers own.\textsuperscript{68} There is a question, however, whether the issue is best addressed by judges or legislators.\textsuperscript{69} Because the principle of exhaustion is conceptually and doctrinally grounded in the common law of property, not copyright statutes, we agree with Perzanowski and Schultz that judges need not feel handcuffed by legislative inaction on the issue.\textsuperscript{70} Moreover, in the United States, policymakers are barely passed the stage

\textsuperscript{66} \textit{Galerie d’art du Petit Champlain inc v Théberge}, 2002 SCC 34 at para 31.
\textsuperscript{69} Maria A. Pallante, “The Next Great Copyright Act” (2013) 36:3 Columbia Journal of Law and the Arts 315.
of public consultation.\textsuperscript{71} In Canada, the word exhaustion does not even appear in the Government’s short, medium or long-term plan for copyright reform.\textsuperscript{72} Given the glacial pace and highly political nature of copyright law reform, and the number of other issues requiring Parliament’s attention, legislative reform seems unlikely anytime soon. So, meanwhile, the Canadian judiciary will likely have to decide whether the nature of digital property will always prevent its resale or, in light of functional equivalence, the doctrine of exhaustion should apply equally to digital and tangible works. In our view, a functionally neutral approach — i.e. treating different technologies differently, not identically — is necessary in order to achieve substantive equality between real space and cyberspace transactions involving the resale of (digital) property.

(b) Testamentary dispositions

User agreements that prohibit the transfer of digital property have been particularly problematic upon death. In Canada, there are no specific laws which empower executors to access a testator’s digital property. If, as Easterbrook’s argument would suggest, the Courts apply general principles of succession law to cyberspace, then digital property should still be divided amongst the estate. If the asset is not specifically bequeathed, then it is distributed as a part of the residue, and if an individual dies intestate, then the asset should be divided according to the rules of succession.\textsuperscript{73} Is a different rule warranted for digital estates?

Bequeathing digital assets is not necessarily as simple as applying general property principles; distributing digital property has significantly complicated testamentary dispositions. Not only do many end user licensing agreements prohibit the transfer of the digital property, but many beneficiaries do not have the passwords required to access the accounts containing the digital assets. For example, one widow made headlines when she attempted to retrieve her deceased husband’s Apple ID password so that she could play games on her iPad. She provided Apple with the serial numbers to the devices, a notarized death certificate and her husband’s will, where he bequeathed the estate to his wife. Apple still refused the request and recommended that Bush acquire a new Apple ID account. Unfortunately, this would mean that all of the music, games and other media previously paid for would need to be repurchased. She later


\textsuperscript{73} In Ontario, for example, the Succession Law Reform Act, 1990 RSO c S 26.
exclaimed, “I could get the pensions, I could get benefits, I could get all kinds of things from the federal government and the other government. But from Apple, I couldn’t even get a silly password.”

The password problem is not only relevant to digital media accounts, but it extends to a variety of situations such as accessing money in PayPal accounts, or ensuring that electronic bills are paid. Testators may attempt to ensure their passwords are provided to their beneficiaries by keeping a hard copy of listed accounts and passwords that can later be provided to their successors. However, the problem with this approach is twofold. First, it might be difficult for an individual to trust someone with their personal information before they die. Second, even if one were to find a trusted confident, passwords often change, and it could be onerous to upkeep a physical list of accounts. This issue has given rise to a variety of digital estate planning agencies. For example, Deadman’s Switch allows for emails to be sent to a beneficiary after the testator’s death, thereby allowing a testator to electronically provide his successors with account information and passwords. SafeSecure not only provides similar password services, but this organization also offers to destroy electronic material that testators would like eliminated after they die. Even Google has attempted to provide tools for digital succession planning by allowing its users to designate a secondary account holder if their account is not activated for 60 days. In this way any emails or electronic documents stored on a Google Drive account can be accessed by successors.

Although these services provide a means for people to plan their digital affairs after death, what if a person dies without accounting for life in cyberspace? Should courts treat digital property as tangible property and apply real space succession law to a digital world? Or, is this a problem that can only be remedied by legislative reform? Similar questions are posed regarding whether one can electronically designate beneficiaries for savings plans and insurance policies. Usually these designations need to be signed and in writing. Given that the aforementioned UECA permits electronic contracts with electronic signatures,

---

74 Rosa Marchitelli, *Apple demands widow get court order to access dead husband’s password*, CBC, online: (January 18, 2016) <http://www.cbc.ca>.
77 Bob Rankin, [RIP] Digital Estate Planning, online: (February 24, 2016) online: http://askbobrankin.com/rip_digital_estate_planning.html>.
one might think that beneficiary designations would also be acceptable. However, the UECA excludes wills and codicils.

If courts determine that a beneficiary designation is the same as a will or codicil, then under UECA, electronic beneficiary designation is not permitted. This ambiguity has led to legal reform in several provinces which makes clear that a beneficiary designation is not a will or codicil (so can be done electronically).79 Thus, in those provinces, digital assignment of a beneficiary is permitted. However, Manitoba, New Brunswick and Quebec have yet to follow suit.80

Gregory explains the reason that the UN model law on which the uniform statute excludes testamentary documents: “The concern with these kinds of documents was that they are often created by unsophisticated people, often without legal or technical advice. It was thought that there was too much risk of undetectable fraud or loss of integrity of data unless more specific security measures were provided, more than a uniform and fairly generic statute could give.”81 Other reports have identified that electronic wills may pose a problem because their format (the software with which they are readable or hardware on which there are stored) could become obsolete before the death of the testator, thereby rendering the will inaccessible. It seems in these instances that the most technology neutral solution is to maintain that wills remain in paper form.82 Also, part of the problem with digital succession is that a beneficiary is not just inheriting property (as in money) but is also acquiring information; extensive information about the deceased that is quantitatively greater and qualitatively different than the information that might be gleaned from a collection of offline journals, photographs, documents and so on. It is one thing to inherit a bundle of letters from the deceased’s secret lover. It is another to inherit and immortalize vast collections of searchable electronic records that the deceased had with other people throughout their lifetime.

Although courts in some provinces may use the principle of technological neutrality to fill legislative gaps in digital succession law, in this instance statutory reform seems the best way to clarify the law. The nature of digital property, specifically in relation to privacy, differs from tangible property. Therefore, new statutory schemes may be required to ensure that a testator’s

79 See, for example, Insurance Act, SBC 2012, c 37, ss 7(1); Fair Practices Regulation, Alta Reg 128/2001 s 5.4.
electronic accounts, including all of the private information therein, are dealt with separately in cyberspace and real space.

4. Digital Property and Privacy

We have seen so far how fundamental questions pertaining to digital property are considered in procedural matters, tort actions and transactional contexts. Another area in which digitization raises significant doctrinal and practical challenges is privacy. New cases expanding common law actions for privacy breaches, in particular, intrusion upon seclusion and public disclosure of private facts, are being triggered by digital technologies including the electronic banking systems, e-health records, pornographic websites, social media and more.\(^83\) But this is not merely a doctrinal challenge; there are deeper conceptual issues to grapple with.

Privacy rights have always had a complex relationship with notions of space and place, ownership and control. Indeed, the core concept of privacy has been shaped by reference (or contrast) to the property rights in incorporeal aspects of human expression and the physical geographic locations in which it is reasonable to expect “to be let alone”, to borrow Warren and Brandeis’ seminal words from their 1890 article in the *Harvard Law Review*.\(^84\) The key contribution made by Warren and Brandeis over 125 years ago was to conceptualize the right to privacy as *effectively* similar to, but *doctrinally* and *theoretically* distinct from, property rights.\(^85\) Despite their warning that “the principle which has been applied to protect these rights [of privacy] is in reality not the principle of private property”,\(^86\) it is sometimes difficult to fully separate the concepts.

Challenges are especially apparent in cases where privacy, place and property rights all collide. For instance, courts tend to collapse “territorial privacy” and


\(^85\) “In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed — and (as that is the distinguishing attribute of property) there may some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.” Samuel Warren and Louis Brandeis, “The Right to Privacy,” (1890) 4:5 *Harvard Law Review* 193.

“informational privacy” into a holistic analysis where the facts of a case implicate both, which happens frequently. Territorial privacy focusses on the places where privacy is reasonably expected, most obviously the home and other private dwellings. This aspect of privacy is often considered in criminal law and constitutional jurisprudence, and has been particularly influential in defining the scope of the section 8 Charter right to be free from unreasonable search and seizure. Informational privacy focusses on the data in which privacy is reasonably expected, especially sensitive personal information. This aspect of privacy is also very relevant in criminal and constitutional contexts, but is often considered too in administrative proceedings, such as complaints to provincial or federal privacy commissioners, and in civil litigation, particularly statutory and common law tort actions for invasion of privacy.

In cyberspace, however, the distinctions between location and information collapse. Consider this anecdote from Kang in the Stanford Law Review:

To focus that vague concern, imagine the following two visits to a mall, one in real space, the other in cyberspace. In real space, you drive to a mall, walk up and down its corridors, peer into numerous shops, and stroll through corridors of inviting stores. Along the way, you buy an ice cream cone with cash. You walk into a bookstore and flip through a few magazines. Finally, you stop at a clothing store and buy a friend a silk scarf with a credit card. In this narrative, numerous persons interact with you and collect information along the way. For instance, while walking through the mall, fellow visitors visually collect information about you, if for no other reason than to avoid bumping into you. But such information is general — e.g., it does not pinpoint the geographical location and time of the sighting — is not in a format that can be processed by a computer, is not indexed to your name or another unique identifier, and is impermanent, residing in short-term human memory. You remain a barely noticed stranger. One important exception exists: The scarf purchase generates data that are detailed, computer-processable, indexed by name, and potentially permanent.

By contrast, in cyberspace, the exception becomes the norm: Every interaction is like the credit card purchase. The best way to grasp this point is to take seriously, if only for a moment, the metaphor that cyberspace is an actual place, a computer-constructed world, a virtual reality. In this alternate universe, you are invisibly stamped with a bar code as soon as you venture outside your home. There are entities called “road providers,” who supply the streets and ground you walk on, who track precisely where, when, and how fast you traverse the lands, in order to charge you for your wear on the infrastructure. As soon as you enter the cyber-mall’s domain, the mall begins to track you through invisible scanners focused on your bar code. It

88 See, for example, Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
89 See, for example, Personal Information Protection Act, SBC 2003, c 63; and Jones v Tsige, 2012 ONCA 32.
automatically records which stores you visit, which windows you browse, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. For example, the cyber-bookstore notes which magazines you skimmed, recording which pages you have seen and for how long, and notes the pattern, if any, of your browsing. It notes that you picked up briefly a health magazine featuring an article on St. John’s Wort, read for seven minutes a newsweekly detailing a politician’s sex scandal, and flipped ever-so-quickly through a tabloid claiming that Elvis lives. Of course, whenever any item is actually purchased, the store, as well as the credit, debit, or virtual cash company that provides payment through cyberspace, takes careful notes of what you bought — in this case, a silk scarf, red, expensive.90

Several recent Canadian cases help explain the relationship between digital property rights and privacy. Some cases combine territorial and informational privacy, such as cases about the collection by or for police of information (like electricity usage or heat emissions) about things happening in someone’s home (like growing marijuana).91 And sometimes, geographic location is the private information, such as data gleaned from smartphones, car navigation systems or other geo-location devices.92

Other cases deal more directly with privacy rights in cyberspace. R v Spencer is a good example. Mr. Spencer was accused of using LimeWire, a peer-to-peer file sharing application, to obtain and share child pornography. The policy learned of his identity by connecting his IP (Internet protocol) address with account information requested from his Internet service provider. The Supreme Court held that there is a reasonable expectation of privacy in subscriber information that could be used to link an identifiable individual with his online activities. Notably, although the Court stated that the analysis “turns on the privacy of the area or the thing being searched”93 it did not consider whether or how the idea of cyberspace as a place might inform the analysis. The trial and appellate courts took differing views on whether the subject of the search was “simply generic information” or “core biographical data”, with the Supreme Court characterizing it as the latter.94

The Court took notice of the fact that “the Internet has exponentially increased both the quality and quantity of information that is stored about

Internet users." But none of the judges at any level considered how transacting in cyberspace fundamentally challenges our understanding of public and private spaces, in the manner contemplated by Lessig, Kang and other cyberlaw scholars. “[B]ecause the computer identified and in a sense monitored by the police was in Mr. Spencer’s residence, there is an element of territorial privacy in issue,” wrote the Court. “However, in this context, the location where the activity occurs is secondary to the nature of the activity itself. Internet users do not expect their online anonymity to cease when they access the Internet outside their homes, via smartphones, or portable devices.”

This insight from the Supreme Court merely hints at a more deeply nuanced understanding of the nature of privacy interests in cyberspace and other emerging digital environments. True, the constitutional right to privacy “protects people, not places.” But to remain technology neutral in a substantive rather than formal sense, the radical innovations the world is witnessing, from smartphones to drones, require shifting the boundaries of the most sacrosanct territorial privacy rights into places beyond the buildings we call home. That point has not yet been fully embraced by courts. Scholars, however, have thought about how “the law could construct a legal fiction of online locales through which territorial privacy, ultimately, could be integrated into cyberspace privacy policy at large.”

Courts have considered the intersections among privacy and personal property. For example, in *R v Patrick*, the Supreme Court held that abandoning personal property by putting it in garbage bags for collection at the front of one’s home forfeits any objectively reasonable expectation of privacy. Issues of personal property and privacy also arise in the digital context. Is there a material distinction between a computer hard drive and the information stored on it? The Supreme Court of Canada case of *R v Cole* suggests that there is. When a computer technician found nude and partially nude images of an underage female student on a high school teacher’s work

---

95 “Browsing logs, for example, may provide detailed information about users’ interests. Search engines may gather records of users’ search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns. “Cookies” may be used to track consumer habits and may provide information about the options selected within a website, which web pages were visited before and after the visit to the host website and any other personal information provided.” *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 at para 46.
computer, the employer copied the contents and provided those to police. The Court found this search was warrantless and unauthorized. There is a distinction between the employer’s ownership of the computer and the employee's reasonable expectation of privacy in the information on the computer. Although the evidence was not excluded, because its admission did not bring the administration of justice into disrepute, this case shows the need to be conscious of the nuances of ownership, control and access of digital property.

A public dispute between Apple and the FBI about access to information contained on a terrorist’s iPhone similarly highlights the distinction between devices and information stored on them. The FBI obtained the physical device, but for a time could not access the password-protected information. It sought a court order to compel Apple’s cooperation, which Apple refused.\footnote{In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No ED-15-0541M (Cal, CD, February 16, 2016) online: (February 16, 2016) <https://assets.documentcloud.org/documents/2714001/SB-Shooter-Order-Compelling-Apple-Assistance-Iphone.pdf>.

The legal case was discontinued when the FBI eventually developed its own technical solution to hack the phone.\footnote{In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, ED No CM 16-10 (SP) (Cal, CD, March 28, 2016) online: (March 28, 2016) <http://pdfserver.amlaw.com/nlj/FBI_apple_20160328.pdf>.} However, a judicially compelled disclosure in a separate matter where the FBI also sought access to information on an iPhone reveals at least a dozen more cases, and that is just cases involving Apple.\footnote{In re Order Requiring Apple Inc to Assist in the Execution of a Search Warrant Issued by the Court, No. 15-MC-1902 (NY, ED, February 29, 2016), online: (February 17, 2016) <http://pdfserver.amlaw.com/nlj/apple_allwrits_list.pdf>.

We anticipate many more controversial disputes like this in the future.

Although these examples are in the realm of criminal law and focus on the application of section 8 of the \textit{Charter}, these constitutional cases also have implications for privacy and digital property rights in the context of civil litigation. One example is \textit{Anton Pill} orders. Counsel and judges must be clear when seeking or granting such orders whether they pertain to the physical objects or the information embodied in them.

Orders compelling discovery from third parties to learn the identity of defendants, i.e. \textit{Norwich} orders,\footnote{\textit{Norwich Pharmacal Co} v \textit{Customs \\& Excise Commissioners} (1973), [1974] AC 133, [1973] 2 All ER 943 (H.L.).} are another context in which the criminal and constitutional law jurisprudence impacts civil litigators. For example, in \textit{Warman v Wilkins-Fournier} — a defamation action where disclosure of identifying details about anonymous online commenters was sought from third-party Internet service providers — the Ontario Superior Court of Justice
held that Charter values inform the interpretation and application of the Rules of Civil Procedure. Similar issues arise in the context of actions against yet-to-be-identified “Doe” defendants in actions for online copyright infringement.

5. Jurisdiction over Cyberspace

One of the earliest practical questions emerging from the Easterbrook/Lessig debate about cyberlaw concerned jurisdiction on and over the Internet. Yet the jurisdictional geography of cyberspace remains unsettled. Charting is, in our view, also among the most pressing of digital property issues for future resolution.

Should standard principles of conflicts and private law apply, or is a more nuanced approach necessary? In his Harvard Law Review article, Lessig correctly pointed out that the nature of cyberspace is inherently different from real space. In real space one must always “be” in a specific geographical location whereas in cyberspace one can simultaneously “be” in multiple locations. While not a matter of digital property rights per se, jurisdictional questions have often been answered by reference to the places with which online actors are connected. Rules of property law, as well as the metaphorical rhetoric of property, are relevant in that context.

Geist was one of the first scholars to grapple with the complexities of Internet jurisdiction. In an article stemming from working supported by the Uniform Law Conference of Canada, Geist critiques the evolving legal tests for asserting jurisdiction over online activities. “While the foreseeability/reasonableness standard may have functioned effectively in the offline world,” notes Geist, “there are several reasons why the Internet complicates the issue.” Among these are the jurisdictional uncertainties which global communications exacerbate, and the temptation for multiple courts to simultaneously assert jurisdiction based mainly on an activity’s local effects. Initially, courts tried dividing cases on the spectrum between passive and active websites, asserting jurisdiction over only the latter. When this false dichotomy became unworkable, courts looked at the effects not just the nature of online activities. A better approach, according to Geist, would be to apply a three-factor test, examining parties’ intentions as manifested through contracts.

---

105 Warman v Wilkins-Fournier, 2010 ONSC 2126, (Div Ct).
109 Ibid at 1356.
technology, and knowledge, to assess jurisdiction claims in cyberspace. Physicality of a party’s presence in a jurisdiction, such as with office space, web servers or other assets, is not among the key factors Geist highlights.

The Supreme Court of Canada had the chance to consider the relevance of territorial connections and digital property rights in the seminal case of *SOCAN v CAIP*. The case raised issues of copyright liability and royalty payments for the communication of music online. A collective society representing copyright owners wished to collect royalties from the Internet service providers who facilitate online transmissions. The administrative tribunal hearing the matter, the Copyright Board of Canada, held that passive Internet intermediaries cannot be liable for the content flowing through their networks. The Supreme Court of Canada agreed.

On the question of where Canadian copyright law applies, the Board would have adopted a test based on the geographic location of the computer server from which music is sent. The Supreme Court instead applied the “real and substantial connection” test, which is generally applicable in conflicts of laws cases. “The Internet ‘exists’, notionally, in cyberspace” acknowledged Justice Binnie, writing for the majority. Citing examples such as hate speech, Internet gambling, cyber-libel, child pornography and e-commerce, Justice Binnie positioned the copyright issue “against the much larger conundrum of trying to apply national laws to a fast-evolving technology that in essence respects no national boundaries.” Failing to acknowledge that cross-border communications online occur at least where the recipient is located, and perhaps elsewhere too, “would have serious consequences in other areas of law relevant to the Internet”, he held.

The Supreme Court was not bothered by the possibility of overlapping liabilities in multiple territories. It held this approach is consistent with general legal principles and international copyright practice; and if it were a problem, the solution is an international treaty, not straining to find a “jurisdictional infirmity”. In a strongly worded dissent, Justice LeBel argued that focusing on the physical location of the server from which music is transmitted would be simpler, better accord with the principle of territoriality in international copyright law, and better protect privacy by not requiring intermediaries to monitor online communications.

---

112 Ibid at para 2.
113 Ibid at para 41.
114 Ibid at para 45.
115 Ibid. at paras 76, 78.
The most recent, and perhaps most difficult, Canadian case to arise on the issue of jurisdiction in cyberspace is *Equustek v Google*. The case is complicated by the fact that it involves a remedy requested against an innocent third party, not the alleged wrongdoer. The plaintiffs, who design, make and sell industrial networking equipment, brought action against former partners for trademark infringement and the theft of confidential information. After civil litigation was commenced, the defendants transformed themselves into a “virtual company”, operating outside of British Columbia but continuing to advertise and sell products in the province. \(^{116}\) While this violated several interlocutory orders of the British Columbia Supreme Court, the plaintiffs’ most (or only) effective remedy was to ask Google to remove the defendants’ allegedly infringing websites from its Internet search and indexing services.

Initially, Google voluntarily delisted several hundred web pages, although only for searches initiated from Google’s “.ca” domain. The plaintiffs were unsatisfied with the extent to which Google was willing to censor search results, and so requested an injunction compelling Google to block access to a schedule of websites including all subpages and subdirectories. The British Columbia Supreme Court granted the injunction. \(^{117}\) The British Columbia Court of Appeal dismissed Google’s appeal. The Supreme Court of Canada granted leave to appeal. \(^{118}\)

The case engages challenging questions about constitutional limits on the territorial jurisdiction of provincial courts, as well as comity and other conflicts of laws principles. For this article, however, some of the most pertinent discussion regards the provincial courts’ *in personam* jurisdiction over Google. As put by the Court of Appeal, Google claimed “it does not have a physical presence in British Columbia, by which it means that it does not have offices or resident staff here, and that none of its servers are located in the Province.” \(^{119}\) In support of this proposition, Google cited the reasons of Justice LeBel in *Van Breda v Village Resorts Ltd.*, which suggested something more than virtual presence is required to assert jurisdiction but expressly disclaimed ruling on the relevance of “e-trade”. \(^{120}\) The chambers judge had rejected Google’s argument that “some form of actual, not virtual, presence is required” for it to be subject to the jurisdiction of courts in British Columbia. \(^{121}\)

---


\(^{118}\) *Google Inc v Equustek Solutions Inc*, 2016 CarswellBC 397 (SCC).


\(^{120}\) *Club Resorts Ltd. v Van Breda*, 2012 SCC 17, [2012] 1 SCR 572 at para 87.

\(^{121}\) *Equustek Solutions Inc v Jack*, 2014 BCSC 1063 at para 34, aff’d 2015 CarswellBC 1590 (CA), leave to appeal allowed 2016 CarswellBC 397 (SCC).
While the chambers judge grappled with the challenges of jurisdiction on the Internet, she quoted language from one of the numerous scholarly papers on point. Comparing e-commerce to the traditional analogue world, Meehan explains: “The geography of the digital world of the Internet, however, is not as easily charted. . . Traditional principles of international jurisdiction, particularly territoriality, are poorly suited for this sort of environment of geographic anonymity.”  

The Court of Appeal did not dispute the notion that asserting jurisdiction over online activities could be controversial, but took comfort in the belief that courts in other countries do not find website blocking orders with extra-territorial effects “unnecessarily intrusive or contrary to the interests of comity.”

Recall that the Ontario Court of Appeal’s decision in *Tucows.Com Co v Lojas Renner SA* also arose from a procedural question of jurisdiction. The jurisdictional issue in *Tucows.Com Co v Lojas Renner SA* is not exactly the same as the issue in *Equustek Solutions Inc v Jack*, but they are related. Whereas *Tucows* involved the extra-territorial service of pleadings, *Equustek* concerns the extra-territorial applicability of an injunction. Both cases consider fundamental matters of civil procedure. *Tucows* relates to Ontario’s *Rules of Civil Procedure*, while *Equustek* turns on British Columbia’s *Court Jurisdiction and Proceedings Transfer Act*.

In reaching their respective decisions, the Ontario and British Columbia appellate courts considered the relevance of digital property differently. In *Tucows*, the Ontario Court of Appeal held that service could be made outside of the jurisdiction because of the fact that the matter involved property (the domain name) in Ontario. In *Equustek*, the British Columbia Court of Appeal

---


held that an injunction has effect outside of the jurisdiction despite the fact that the respondent, Google, did not hold property in British Columbia. Indeed, the injunction against Google significantly impacts its property (servers, domains and other assets) outside the jurisdiction.

6. Technological Regulation of Digital Property Rights

Before concluding, there is a final point to mention: Private parties are increasingly fencing off cyberspace with technological measures that replicate real-space geographic and jurisdictional boundaries. One practical example is geo-fencing, used by companies like Netflix, Spotify and other content providers to segment markets. In the early days of cyberspace, companies like iCraveTV tried to prevent extra-territorial access to content through click-wrap agreements, requiring users to contractually attest to their geographic location. Now, using technological measures that detect Internet users’ geographic location from their IP (Internet protocol) addresses, providers can block access to content outside of any particular territorial jurisdiction. They may do so for legal reasons, for instance because copyright licenses tend to be geographically limited in scope. Another legal reason may be to demonstrate an intention not to do business in a particular place, so as to avoid the potential of litigation in that jurisdiction. They may also do so for economic reasons, for instance, to price discriminate between consumers in rich and poor countries.

The long-term implications of this practice are not clear, yet Internet policymakers have rushed to reinforce geo-fences. Despite cautious warnings, they have done so under the guise of protecting copyright to, among other things, “better address the challenges and opportunities of the Internet” and “ensure that it [the Copyright Act] remains technologically neutral.” Reforms to the “Civil Remedies” section of the Copyright Act, enacted in 2012, make it illegal to “avoid, bypass, remove, deactivate or impair” any “technology device or component” that “controls access” to content.

General civil litigators and provincial court judges are not immune from dealing with anti-circumvention cases. Although digital copyright matters very often arise in administrative proceedings and federal courts, they are also cropping up elsewhere. A recent case in Ontario’s Superior Court of Justice, 126 National Football League v TVRadioNow Corp, 53 USPQ 2d 1831 (WD Pa, 2000). Michael Geist suggests the use of technology to target or avoid a particular jurisdiction should be a key factor in determining whether or not to assert jurisdiction over a cyberlaw matter. Michael Geist, “Is There a There There: Toward Greater Certainty for Internet Jurisdiction,” (2001) 16:3 Berkeley Technology Law Journal 1345 at 1401.


Copyright Modernization Act, SC 2012, c 20.

Copyright Act, RSC 1948 c C-42, s 41-41.1.
Ottawa Small Claims Court, illustrates the proverbial tip of the iceberg. The surprising and unprecedented decision in 1395804 Ontario Limited (Blacklock’s Reporter) v Canadian Vintners Association proves the dangers of naively arguing and/or adjudicating digital property issues. The defendant in the case had done nothing but receive and read an email from a third party. Attached to the email from the third party was a news report prepared by the plaintiff in which the defendant was quoted. On these facts, the deputy judge found the defendant liable for copyright infringement and for circumventing a technological protection measure, i.e. the paywall that controlled access to the digital content (to which the third party had paid for lawful access). The decision, being a small claims court judgment, is not binding or especially persuasive for any other court or tribunal, but nevertheless raises concerns.

In practice, anti-circumvention provisions that regulate digital property rights are anything but technologically neutral. They inherently discriminate between online and offline activities, granting broader protection in cyberspace than was ever available in real space. For example, the ability to control access to content has never been an exclusive right available to copyright owners offline. But prohibitions on circumventing the technologies through which content distributors restrict access have, in effect, created a unique digital right to determine who may watch, hear or read material online.

Moreover, technological protection measures are, in pith and substance, more about matters of property and civil rights than copyright. Serious constitutional questions therefore cloud the validity and applicability of these provisions. Anti-circumvention provisions constrain what owners of devices may do with their personal property and lawfully acquired digital content, and change the way that businesses and consumers contract in the digital environment.

The use of technological measures to privately regulate cyberspace was an issue Lessig foresaw in his seminal work on cyberlaw. In his book Code and Other Laws of Cyberspace, Lessig differentiates between “West coast” and “East coast” code, a metaphor for the laws made in Silicon Valley as compared to Washington. His central thesis — that computer/West coast code is as or

131 1395804 Ontario Limited (Blacklock’s Reporter) v Canadian Vintners Association (October 16, 2015), Gilbert D.J. (Ont. SCJ).
more important than legal/East coast code — is proving true through courts’
difficulties creating truly technology neutral resolutions to digital property
disputes.

III. CONCLUSION

What and where are cyberspace and the digital property rights in it? Those
questions connect each of the doctrinal components of digital property law
discussed throughout this article.

In certain areas, we observe the tendency to treat the digital domain as a
matter of personal property. Although the Ontario Court of Appeal did not
settle whether a domain name is real or personal property, it held that the asset
was indeed property and in either case is “in Ontario” for the purposes of the
Rules of Civil Procedure. In Intel v Hamidi and its Canadian counterpart,
Century 21, courts considering the possibility of a cyber-trespass applied the
doctrine pertaining to chattels not real property, where proof of physical harm is
a requisite part of the action. And most of the civil litigation and legislative
policymaking regarding the transfer of digital property rights has focussed on
personal property issues.

However, the metaphor of cyberspace as place, i.e. a distinct territory where
unique legal issues arise, is shaping other aspects of the law of digital property.
The blurring line between territorial and informational privacy is one example.
The burning jurisdictional question considered in this article is another.
Importantly, no court has suggested (nor should a court suggest) that the
Internet is a jurisdiction unto itself, where the laws of other territories are
inapplicable. Rather, courts are rightly beginning to recognize that cases
involving cyberspace raise distinct policy and practical issues that cannot be
adequately addressed by importing conventional legal doctrine into the digital
realm. Here, technological neutrality means something more.

Judge Easterbrook’s approach is essentially the bare “media neutrality”
perspective that informed early views in e-commerce and copyright law about
what technological neutrality is: The law should be applied the same way
regardless of the technological context. A more sophisticated approach to
cyberlaw, on the other hand, reflects a richer vision for technological neutrality;
one that considers substantive functional equivalence. This aligns with the way
scholars such as Craig and Kerr have independently described the application of
this principle in the contexts of digital copyright and artificial intelligence,
respectively. When dealing with digital property, we endorse this more nuanced
approach as something to strive for in the civil litigation system.

The mere principle of media neutrality — formalistically transposing
orthodox property rules into digital disputes — is insufficient. Rather, civil

litigators, adjudicating courts and cyberlaw-makers should aim for functional equivalence. That does not mean we always support technological exceptionalism. In many cases, media neutrality may suffice. But in many other circumstances, issues triggered by the Internet truly are different, and deserve to be treated as such. Twenty years of experience has shown that cyberlaw is not “the law of the horse”, as Judge Easterbrook claimed. We believe digital property rights issues warrant a more nuanced analysis than they have thus far received in civil litigation.