Message from the Chair

Dear Cyberspace Colleagues:

I am pleased to announce that our 2019 Cyberspace Law Institute and Winter Working Meeting will be in St. Petersburg, Florida on January 25-26. Stetson University College of Law will be graciously hosting us, and the official hotel (still to be finalized) will be on St. Pete Beach—just 5-10 minutes away by Uber/Lyft or rental car! More details will be available soon. For now, please save the dates. The institute and meeting will follow a similar format as in the recent past with CLE programs, subcommittee meetings, and roundtable discussions. If you would like to propose a program or roundtable, please see Ed Morse’s article below.

While the BLS Annual Meeting is still a few days away, our committee is already beginning to plan for Spring Meeting, which will take place March 28-30, 2019 in Vancouver, British Columbia. Ed Morse shares below details on how to submit proposals for CLE programs there.

I look forward to seeing many of you in Austin. If you cannot be there in person, please do join us by phone at our committee meeting and any subcommittee meetings. All our meetings are on Thursday, September 13. Here is the link to the searchable schedule with call-in information.

Are you looking to get more involved with the Cyberspace Law Committee? If you would like to take on a leadership role, please let Cheryl Burtzel or me know as we have a few openings for subcommittee vice-chairs and directors who liaise with the Section administrative committees. And if you have an idea for a publication or other project, please share it. Your ideas and involvement with the committee’s work are always welcome!

Safe travels to Austin. The margaritas, chips, and guac are waiting!

Cheryl Dancey Balough
Chair, Cyberspace Law Committee

Subcommittee News

From the Cloud and Enterprise Technology Subcommittee

Please join the Cloud and Enterprise Technology Subcommittee in Austin as we jump start a book project with a working session to review a sample chapter for content and format. The Directors’ Legal Handbook - Enterprise Technology project will be a great opportunity to contribute as author, editor, or reviewer. A draft outline is posted in the "Related Resources" section of the subcommittee page.

From the Current Law Task Force

Current Law Task Force Meeting - September 12

Are you interested in writing about emerging topics in cyberspace law? Would you like to publish a piece on a recent development, but don't have the time to draft a
long article? Are you looking for a way to get more involved with the Cyberspace Law Committee without traveling to a meeting?

If so, call in to the next meeting of the Cyberspace Law Committee's Current Law Task Force on September 12 at 10:00 am CT/11:00 am ET. New members are always welcome.

The Current Law Task Force tracks and reports on recent developments in cyberspace law and serves as an incubator for publications and presentations. There are a variety of available publication opportunities, including contributions to the Cyberspace Law Committee Newsletter and Business Law Today. The Task Force can help you publish works of varying length and detail, ranging from long-form articles to pieces as brief as one paragraph.

The Current Law Task Force meets through monthly conference calls to discuss new developments and ideas for publications. The dial-in information for the call is below:

Call In: 312-667-9356
Conference ID: 079455
Security Pin: 160049

From the Robotics and Artificial Intelligence Subcommittee

The Robotics and Artificial Intelligence Subcommittee is seeking volunteers to help develop programs, webinars, and articles relating to robotics and AI. The subcommittee plans to work with the Healthcare Task Force on legal issues with the use of robotics in healthcare. Other subcommittee topics include use of robotics in the commercial/industrial space, such as delivery vehicles, drones, and their overall integration with the IoT platform, and weaponization of robotics. Other ideas and topics also are welcome.

If you are interested in these topics, and want to participate, please attend the subcommittee meeting in Austin on Thursday, September 14 at 11:30 a.m. If you cannot attend the meeting in person, please join us by phone (see link above for call-in information) or contact subcommittee co-chairs Lisa Lifshitz or Richard C. Balough.

Call for CLE Program Proposals

As the Annual meeting in Austin looms larger on the horizon, we need to remind you about two future events to put on your planning calendar. Both events present opportunities for CLE programming, and we invite you to submit proposals for either or both events.

First, the Business Law Section’s Spring Meeting will be held on March 28-30, 2019, at the Vancouver Convention Center Fairmont Waterfront, Pan Pacific and Vancouver Marriott Pinnacle in Vancouver, BC. As this year's Spring Meeting occurs a little earlier in the calendar year than in the past, planning for CLE programming must begin early. We are requesting proposals for CLE programs at the Spring meeting by Saturday, September 15, 2018, so that we can coordinate submissions on behalf of the committee. This date should allow you to discuss proposals at your subcommittee meetings in Austin.

Second, our Committee will hold its annual Cyberspace Law Institute and Winter Working Meeting (“CLI/WWM”) on January 25-26, 2019 in St. Petersburg, Florida. The 2019 CLI/WWM will follow a format similar to past meetings, including CLE programs, working sessions for subcommittees to address new projects, and roundtable discussions of current topics. Please start thinking about:
1. Topics for potential CLE presentations;
2. A roundtable discussion topic you would like to lead;
3. Projects worthy of attention in your subcommittee sessions (which can also be discussed at the annual meeting in Austin); and/or
4. Any suggestions you may have for a luncheon speaker.

Your proposals for CLE programming should include:

- A proposed title
- A program chair
- Key topics to be addressed
- Potential panelists (which can reflect positions rather than names)
- Co-sponsorship potential (for Spring meeting only)

Keep in mind that niche programs are welcome for the Cyberspace Law Institute, which has a target audience likely to be more interested in detailed cyberlaw topics, including technical discussions of relevant technology. Also note that we are looking for shorter programs for the CLI/WWM, generally targeting 20-45 minutes (vs. 60-120 minutes for the Spring meeting). We would like your proposals for the CLI/WWM by **Friday, October 12, 2018**.

Again, proposals for the Spring meeting are due on or before **September 15, 2018**. Proposals for the Cyberspace Law Institute/Winter Working meeting are due on or before **October 12, 2018 (CLI/WWM)**. Of course, feel free to contact Ed Morse or Cheryl Burtzel with any questions.

**Call for Proposals: Internet-related Topics**

Cyberspace Law Committee members Sharon Sandeen and Michael Fleming have passed along the following information about a symposium titled *Revisiting "Realizing the Information Future: The Internet and Beyond," the Good, the Bad, and the Ugly*. The symposium organizers are very interested in hearing from practicing lawyers with interest in the topics (as well as traditional academics). The symposium will be held at Mitchell Hamline School of Law and Hamline University in St Paul, MN on Friday, March 29, 2019 (which unfortunately conflicts with the Business Law Section Spring Meeting).

Per the organizers: "We invite you to submit an abstract of a paper topic to present at a cross-disciplinary symposium organized by the Intellectual Property Institute at Mitchell Hamline School of Law and the Center for Justice and Law at Hamline University to be held on Friday, March 29, 2019 in St. Paul, Minnesota. The symposium is intended to explore the issues raised in the report ‘Realizing the Information Future: The Internet and Beyond,’ published by National Academy Press in 1994, and how the commercial use of the internet has changed our world since 1994.” The full invitation can be found [here](#). Note that paper abstracts are due by October 19, 2018.

**Blockchain and the Uniform Electronic Transactions Act**

*By A.J. Bosco, StoneTurn*

I. Introduction

Since the first mention of "blockchain" in the 2008 white paper attributed to Satoshi Nakamoto, it has grown from an obscure concept developed to facilitate Bitcoin transactions to a technology that has scores of current and predicted use cases beyond digital currency.
Despite its growing acceptance, there is no universally accepted definition of blockchain. There are, however, certain elements common to most blockchains. Most basically, it is a digital database consisting of a continuously growing list of records, called blocks. These blocks of data are chained together using cryptography, making it difficult to rewrite the older records. Further, a blockchain and the data on it can be simultaneously used and shared within a large, decentralized, publicly available network. Importantly, it allows information to be stored and exchanged without any central authority or need for third-party verification.

Read more…

Canadian Privacy Commissioner Says Public Profiles Are Private

By Imran Ahmad, Katherine Barbacki, Alexia Magneron, Miller Thomson LLP

On June 12, 2018, the Office of the Privacy Commissioner (“OPC”) released its report into Profile Technology Ltd.’s (“Profile Technology”) use of “publicly available” Facebook profiles. The OPC concluded that Profile Technology had not obtained the necessary consents from individuals whose Facebook profiles they were collecting for the purposes of establishing its own social networking website. The case is an important one since it sheds light on what limits may be imposed by Canadian privacy regulators on the use of personal information that may be available to the public from time-to-time on social networking platforms.

Read more…

Federal Court Considers the Garnishment of Cryptocurrencies to Satisfy Judgment

By Stephen T. Middlebrook, Womble Bond Dickinson

In what appears to be the first opinion dealing with the collection of a judgment where the defendant owns cryptocurrency, Judge Fox of the Eastern District of Michigan considered a motion requesting that the Court direct Coinbase to liquidate the defendant’s accounts and distribute the proceeds to the plaintiff.

Ultimately ruling that the plaintiff erred procedurally (since the judgment should have been registered in the defendant's domicile-New York), the Court reasoned that the defendant's cryptocurrency was intangible property and could be used to satisfy the judgment; the plaintiff just needed to follow the rules. Assuming other courts follow this reasonable and intuitive approach, the belief that cryptocurrency provides protection against judgments (as has been argued by some) may not be well-supported.

DHS Hosts Election Security Event

By Heidi Kuffel, Skarzynski Black LLC

The Department of Homeland Security recently hosted a three-day event focusing on cybersecurity and potential cyber incidents that could impact elections. Participants from 44 states, D.C., various public agencies, including the FBI and U.S. Cyber Command attended the event, which used tabletop simulation in order to allow the participants to discuss and understand various risks specifically
surrounding elections, including manipulation of social media and news, infections of voting machine through malware, and spear phishing campaigns. The goal of the exercise was to increase communications of all those involved in the election process, to strengthen the ability to recognize potential cybersecurity threats, increase familiarity with the process of requesting support from various resources in the event of such a threat, and analysis of general best practices in responding to a cyber incident, including the significance of a well delineated response plan.

For more information on the exercise hosted by the DHS on election security, click here.

**Committee Member News**

Sarah Jane Hughes submitted an invited Symposium article to the Cleveland-Marshall Law Review - *Conceptualizing the Regulation of Virtual-Currency Providers*. She previously participated as a panel member at their April 6, 2018 symposium on the blockchain and virtual currencies.

**Call for Future Contributions**

Do you have something that might make a good contribution to next month's Cyberspace Law newsletter? Email Tom Kierner with your blurb! Have a less Cyberspace-y contribution? It might be a good fit for Business Law Today. Email Juliet Moringiello, and she will help you with the submission process.
Blockchain and the Uniform Electronic Transactions Act

By A.J. Bosco*

I. Introduction

Since the first mention of “blockchain” in the 2008 white paper attributed to Satoshi Nakamoto, it has grown from an obscure concept developed to facilitate Bitcoin transactions to a technology that has scores of current and predicted use cases beyond digital currency.

Despite its growing acceptance, there is no universally accepted definition of blockchain. There are, however, certain elements common to most blockchains. Most basically, it is a digital database consisting of a continuously growing list of records, called blocks. These blocks of data are chained together using cryptography, making it difficult to rewrite the older records. Further, a blockchain and the data on it can be simultaneously used and shared within a large, decentralized, publicly available network. Importantly, it allows information to be stored and exchanged without any central authority or need for third-party verification.

One result of there being no broadly accepted definition of blockchain is that state legislators have little guidance when considering laws that affect blockchain. Consequently, as states begin to pass blockchain friendly laws they are using different, and sometimes conflicting, definitions of blockchain, or no definition at all. This dilemma is particularly acute within the context of the Uniform Electronic Transactions Act (“UETA” or the “Act”), which states are amending as a sign that they are a welcoming environment for blockchain commerce.

The UETA “establishes the legal equivalence of electronic records and signatures with paper writings and manually-signed signatures, removing barriers to electronic commerce.” The drafters of the UETA made clear that its objective is very limited: to provide that “an electronic record of a transaction is the equivalent of a paper record, and that an electronic signature will be given the same legal effect, whatever that might be, as a manual signature.”

According to the Uniform Law Commissioners, the most fundamental rule contained in the Act provides that a "record or signature may not be denied legal effect or enforceability solely because it is in electronic form.”

These rules resulted in the following relevant statutory definitions:

“Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

“Electronic record” means a record created, generated, sent, communicated, received, or stored by electronic means.

“Electronic signature” means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

“Record” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

As of August 2018, three states—Arizona, Nevada, and Tennessee—have amended the UETA to specifically make records maintained on a blockchain electronic records within the meaning of the UETA. Three additional states—Florida, Nebraska, and Ohio—have introduced, but not yet passed, blockchain-related UETA legislation. Each of these states’ proposed legislation contains
a definition of blockchain. Two additional states—Illinois and New York—which have not adopted the UETA - have proposed laws that define blockchain in connection with electronic records and signatures.

The eight states that have enacted or are considering legislation bringing blockchain within the scope of electronic records statutes use three definitions of blockchain among them. All give legal recognition to electronic records created, stored, or verified by use of a blockchain. Most of them specify that signatures and records secured by blockchain are electronic records.

Arizona, Florida, New York, Ohio and Tennessee define “blockchain technology” as “distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.”

The laws provides for the legal status of blockchain as follows:

A. A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature.

B. A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record.

In Nebraska and Nevada blockchain mean “an electronic record of transactions or other data which is: (a) uniformly ordered; (b) redundantly maintained or processed by one or more computers or machines to guarantee the consistency or nonrepudiation of the recorded transactions or other data; and (c) validated by the use of cryptography.” It also amended the definition of “electronic record” to mean “a record created, generated, sent, communicated, received or stored by electronic means. The term includes, without limitation, a blockchain.”

Illinois’ proposed bill defines "blockchain" as “an electronic record created by the use of a decentralized method by multiple parties to verify and store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information. "Cryptographic hash” means “a mathematical algorithm which performs a one-way conversion of input data into output data of a specified size to verify the integrity of the data.”

II. Analysis

The purpose of the UETA is to remove barriers to commerce. But the varying definitions of blockchain used by Arizona, Nevada, and Illinois in amending their electronic records laws may create unintended roadblocks.

First, these different definitions could foreseeably impede commerce by making a formerly universal law not so universal. Records or signatures created, stored or verified on a blockchain in Nevada may not be valid in Arizona because Nevada does not require blockchains to be “immutable” or to “provide[] an uncensored truth.” A blockchain that meets Tennessee’s definition might not be recognized in Nevada because it might not “guarantee the consistency or nonrepudiation” of the transactions or data recorded on it. Or, a company from a jurisdiction that does not define blockchain may have trouble establishing that its blockchain-maintained records are valid in Illinois because its “cryptographic hash” algorithm fails the definition proposed by Illinois. And, if New York passes the proposed legislation, a non-New York business engaged in
commerce there may find its use of smart contracts limited to those that “take custody over and instruct transfer of assets.”

Second, blockchain technology is still new and developing. Tomorrow’s blockchain may well be different from today’s. Legislators in Arizona, for example, cannot be sure that the detailed, specific, and prescriptive definition they have enacted into law, which includes the descriptors “immutable” and “uncensored truth,” will fit the blockchain of the future. A litigant may be able to prove that an electronic signature recorded on a new type of distributed ledger technology is not covered by Arizona’s amendment to the UETA because the newly created ledger does not fit Arizona’s definition of blockchain. Consequently, these amendments may nullify the purpose of amending the UETA, which is to ensure that records kept on a blockchain are accepted as electronic records.

Third is a matter of accuracy. The description of blockchains as “immutable” may not be entirely accurate. While expensive and time consuming, many countries could afford to create a “51% attack” on a blockchain (a 51% attack on a blockchain refers gaining control of more than 50% of a network’s computing power), such as Bitcoin, blocking verification of new transactions or reversing previously confirmed transactions. Furthermore, a global consulting firm has developed and patented a technique to modify existing blockchain technology to allow designated authorities to edit, rewrite or remove previous blocks of information without breaking the chain. Also, blockchains have been known to fork. In 2013 and 2017, the Bitcoin blockchain forked into two separate blockchains, when the network accepted one new block as valid while another part rejected it and accepted a different block, meaning that two separate, incompatible ledgers of Bitcoin transactions existed simultaneously. Further, “immutable” may not always be a desired quality, as it implies a record will last forever, or at least indefinitely. This permanence could cause risk management headaches for companies that have document control policies requiring that records be periodically destroyed. Perhaps even more concerning is that an immutable record could run afoul of the right to be forgotten contained in the European Union’s General Data Protection Regulation.

Fourth, the statutory assertion that blockchain provides “an uncensored truth” is questionable. Using the Merriam-Webster definition of uncensored as “not having any part deleted or suppressed” implies that the drafters of the legislation believe data on a blockchain cannot be removed or hidden, and consequently, must be true. If data maintained on a distributed ledger provides “an uncensored truth,” it implies information secured through blockchain cannot be challenged in states that use this definition of blockchain.

Finally, recall that in advocating for the UETA, the Uniform Law Commissioners stated that the most fundamental rule contained in the Act is "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form.” Simply put, records maintained on a blockchain are manifestly “electronic records” under the UETA. Indeed, the Illinois and Nevada definitions of blockchain includes the words, “an electronic record.” Therefore, they are already within the ambit of the UETA, and so it need not be amended. Businesses that want to engage in commerce via blockchain may be better served in states that choose not to make a big splash in the blockchain pool.
On June 12, 2018, the Office of the Privacy Commissioner (“OPC”) [1] released its report [2] into Profile Technology Ltd.’s (“Profile Technology”) use of “publicly available” Facebook profiles. The OPC concluded that Profile Technology had not obtained the necessary consents from individuals whose Facebook profiles they were collecting for the purposes of establishing its own social networking website. The case is an important one since it sheds light on what limits may be imposed by Canadian privacy regulators on the use of personal information that may be available to the public from time-to-time on social networking platforms.

**Background**

Profile Technology, a New Zealand-based company, had been retained by Facebook in 2007 to provide advanced search functions for its site. Specifically, it indexed the public parts of users’ profiles – in a manner that is similar to how Google and other search engines index information on the internet more broadly. To this end, Profile Technology claimed that it was provided unlimited access by Facebook to information that its users had consented to make public and accessible to search engines.

Profile Technology subsequently used the information that it had collected from Facebook to build its own social networking site, never seeking the consent – implied or express – of the users whose profiles were being migrated and incorporated into its site.

Subsequently, five Canadian individuals filed complaints with the OPC, alleging that Profile Technology had collected and used their personal information without their knowledge and consent. These complainants explained: (i) in certain circumstances, they were unable to have their personal information removed from the website; (ii) the personal information used by Profile Technology was not accurate; and (iii) Profile Technology had inadequate procedures in place to receive and respond to complaints and inquiries about its policies and practices relating to the handling of personal information.

**Findings**

**Profile Technology Did Not Have Users’ Consent**

The Canadian complainants indicated to the OPC that they learned that their information appeared on Profile Technology’s website after they conducted internet searches for their own names.

The complainants pointed out in their claims that Profile Technology never sought their consent for the collection and use of their personal information. Interestingly, Profile Technology argued that such information was “publicly available” and that it was not required to obtain consent of

---

1 Imran Ahmad is a Partner at the Canadian law firm Miller Thomson LLP and leads the Cybersecurity Law Practice. Katherine Barbacki and Alexia Magneron are associates at Miller Thomson LLP focusing on cybersecurity and privacy law.
the users. Further, Profile Technology claimed that Facebook was responsible for obtaining permission to make the information public and available to search engines. It relied on Facebook’s privacy policies from 2009 and 2010 and Facebook’s blog post from 2007 to assert that notice had been given to users that their public information may be found by external search engines.

More specifically, Profile Technology claimed that publicly accessible Facebook profiles should be considered a “publication” under PIPEDA’s Regulations Specifying Publicly Available Information [3] (the “Regulations”). Subsection 1(e) of the Regulations refers to “personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.” Profile Technology submitted that a person who places information on their Facebook profile “publishes” the information, making Facebook profile information a “publication” for the purposes of the Regulations.

The OPC flatly rejected Profile Technology’s assertion that profile information is “publicly available”, such that is exempt from the requirement to obtain consent. Even if the OPC accepted that Facebook users’ consent for its original collection of profile information for the purposes of offering search engine services, it did not have consent to subsequently use that information for purposes of creating and populating its own social networking website. [4]

Not All Public Information is “Publicly Available”

The OPC noted that PIPEDA recognizes that not all information in the public domain will be considered “publicly available”. In this regard, there is an acknowledgment that information that may be in the public domain is still worthy of privacy protection. Treating a Facebook profile as a publication would be counter to the intention of PIPEDA, undermining the control users otherwise maintain over their information at source.

The OPC concluded that the personal information at issue was not publicly available within the meaning of PIPEDA. [5] As such, the respondent was required to ensure individuals’ consent for its use of their personal information copied from Facebook and posted on its website.

OPC Recommendations

The OPC recommended that, among other things, Profile Technology remove from its website and delete from its records, all individual profiles and groups associated with any Canadian (or Canadians), including those associated with the complainants. Profile Technology did proceed with the bulk deletion of Canadian data.

Prior to issuance of the OPC report, Profile Technology had removed the profiles from its website. As of April 1, 2018, the website simply consisted of a notice page titled “Profile Engine has now been donated to the Internet Archive (31st March 2018)”. On April 9, 2018, the OPC observed that the files were becoming increasingly difficult to find via search engines (which had presumably de-indexed the links to the torrent files [6]) but the OPC was still able to find the torrents on the dark web.

Key Takeaways
The OPC’s decision in the Profile Technology case is important given that an increasing number of individuals regularly share their personal information with multiple social networking websites. As these websites become increasingly sophisticated and use third party vendors to get insights about their users (e.g., through the use of analytics), they provide vendors access to their users’ personal information. Implied consent in lengthy privacy policies that very few users read and understand is not sufficient from a Canadian privacy standpoint, as stated by the OPC in its recently released *Guidelines for Obtaining Meaningful Consent*. [7] Accordingly, to the extent that a vendor is relying on the consent obtained by the entity collecting the personal information in the first instance, it should ensure that it has taken necessary steps to demonstrate – e.g., through contractual language – that the requisite consents were obtained for the purposes contemplated by the vendor.

Another key takeaway is that simply because a third party may be able to publicly access an individual’s personal information does not mean that it is “publicly available”, as defined in PIPEDA and the Regulations. In fact, information that may be in the public domain is still worthy of privacy protection and appropriate consents should nonetheless be obtained.

From a jurisdictional standpoint, Profile Technology was unsuccessful in arguing that the OPC had no jurisdiction on that basis of the company not having a physical presence in Canada. PIPEDA has extraterritorial scope if a real and substantial connection can be established. That said, in cases where the OPC’s jurisdiction may be established, enforcement is another matter, one which was not tested in this case. However, the extraterritorial scope issue is likely to be an important topic as the EU’s *General Data Protection Regulation* [8] and the *California Consumer Privacy Act of 2018* [9] both have extraterritorial reach.

---

[1] The Office of the Privacy Commissioner of Canada is an agent of the Canadian Parliament responsible for the protection and promotion of privacy rights. It oversees compliance with the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”), Canada’s federal private-sector privacy law.


[6] A “torrent” is a file that facilitates efficient dissemination of the file via peer-to-peer sharing, whereby any person who “replicates” (i.e., downloads) a file can then “seed” it (i.e., make it available for download by others).
