BUSINESSCLASS
KNOWLEDGE ▪ SEMINARS ▪ INSIGHTS

Blakes

TRENDS

CYBERSECURITY

As part of our quarterly series on current trends across different industries, our first article for 2019 looks at the current landscape of cybersecurity and highlights key legal trends and developments. We also offer some practical advice on what businesses can do to equip themselves and mitigate their risk in this constantly evolving space.

By Joe Abdul-Massih, Imran Ahmad, Catherine Beagan Flood, Hélène Deschamps Marquis, Christopher DiMatteo, Nicole Henderson and Wendy Mee

1

Smart Contracts

Organizations are increasingly experimenting with applications built on blockchain technology. The most advanced and promising application of blockchain technology remains smart contracts. However, many important legal concerns have come to light, particularly with respect to cybersecurity and privacy law.

In its simplest form, a blockchain is a distributed ledger — that is, a list of transactions that is shared among a statistically relevant number of computers. Prior to being added as a block, the integrity of a transaction must be confirmed through a "consensus mechanism" whereby various computers in the network agree to update the blockchain after a transaction has taken place. Once a block is validated and added to the ledger, it cannot be changed unless validated by the entire network, creating a permanent and immutable public record.

Smart contracts are self-executing electronic instructions drafted in computer code, allowing a computer to "read" the contract and automatically execute the stipulations when predetermined conditions are met.

Cybersecurity Challenges

Blockchain technology is often touted as being "secure" given that the data is distributed across many computers, making it difficult, in theory, to be tampered with by an unauthorized third party. However, this does not mean that vulnerabilities in the underlying code cannot be exploited, something that has occurred several times in recent years.

Organizations must be aware of cybersecurity risks before they decide to implement smart contract solutions and take appropriate measures to ensure effective security for the permissioned blockchains they deploy.

One strategy used to maintain the integrity of the ledger is to evaluate the minimum number of miners that could collude and overpower the chain and ensure that the number of legitimate miners is always above this threshold.

Companies should also establish technical and organizational procedures that reduce the potential for vulnerabilities in the system and put in place an emergency plan to be deployed in the event of such a failure.

Privacy Challenges

Privacy laws are designed to regulate a world in which personal information management is centralized and where the controller of such information and defined third parties who merely process the data are clearly identified and accountable. Applying these concepts to a decentralized network such as blockchain, where a multitude of actors control and process the data, requires a careful analysis of the different players involved on a network, especially in the absence of any guidance on the topics by Canadian privacy regulators.

Internationally, the French privacy regulator has provided some guidance. For example, given the immutable and permanent nature of the data stored on the blockchain, there are concerns that certain privacy principles, such as the right to be forgotten, the right to rectification and the right to object to processing, may be irreconcilable with the use of blockchain technology. Attempting to find a middle ground, the French privacy regulatory has recognized that there may be some technological solutions that may allow stakeholders to comply with the EU's General Data Protection Regulation (GDPR). However, these solutions must be assessed on a case-by-case basis.

The key takeaway is that organizations looking to store or process personal information on the blockchain through the use of smart contracts will need to carefully consider what technological solutions they should implement and whether their chosen solutions can withstand regulatory scrutiny.

2 Privacy Class Actions

Since the Ontario Court of Appeal's seminal 2012 decision *Jones v. Tsige (Jones)*, which recognized the tort of "intrusion upon seclusion" in Ontario, privacy class actions have become increasingly commonplace in Canada.

This new tort requires that the defendant intentionally invaded the plaintiff's private affairs or concerns, that a reasonable person would regard the invasion to be highly offensive, and that it caused distress, humiliation or anguish. Where these elements are satisfied, nominal damages of up to C$20,000 may be awarded even if the plaintiff has not suffered pecuniary loss. Intrusion upon seclusion has been recognized as a valid cause of action in several provinces, and others have statutory privacy torts.

Courts have generally been willing to use intrusion upon seclusion as a springboard for certifying privacy class actions, many in circumstances that bear little factual resemblance to *Jones* (an individual case involving a bank employee snooping into financial records). For example, Canadian courts have certified privacy class actions in cases involving: dissemination of intimate images, unintentional loss of electronic

storage media containing personal information and data breaches arising from hacking by criminal third parties.

However, it remains to be seen whether plaintiffs will ultimately be able to recover damages for intrusion upon seclusion or other privacy torts (such as public disclosure of private facts). To date, no privacy class action in Canada has proceeded to a merits determination.

There have been a handful of settlements of privacy class actions. Most have represented fairly low values per claimant. However, 2018 saw some higher-value settlements approved in cases involving deliberate breaches of highly sensitive personal information, such as medical or banking records, and in one case involving the loss of an unencrypted hard drive containing sensitive financial information.

However, there are some signs that Canadian courts may begin applying greater scrutiny to proposed privacy class actions. In *Broutzas v. Rouge Valley Health System*, the Ontario Superior Court of Justice recently refused to certify a privacy class action in which rogue hospital employees allegedly accessed patient records to sell new mothers' contact information as RESP sales leads.[1]

The court held that intrusion upon seclusion could not be established because contact information is not private. The court also clarified that intrusion upon seclusion is a "tight and narrow" tort and is not proved through "guilt by association"; to make out the cause of action, a deliberate intrusion *by the defendant* is required. In addition, the court rejected a proposed negligence claim against several of the defendants, in part on the basis that a negligence claim should not be available as a "backstop" where an intrusion upon seclusion claim could not be made out.

With the coming into force of federal mandatory breach reporting obligations under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), we expect more reporting of privacy breaches and likely more class action activity as a result.

Greater scrutiny of such claims by the courts may follow as judges become more familiar with the context of data breaches and the fact that companies with reasonable security safeguards may nonetheless fall victim to a successful cyber-attack.

3 Privacy Breach Reporting

The reporting of cybersecurity incidents can serve many practical purposes. Notifying affected individuals may allow them to take steps to reduce the risk of identity theft, fraud or other potential harms. Reporting to regulators facilitates regulatory oversight and allows regulators to gather information relating to cybersecurity threats and trends.

As cybersecurity incidents are on the rise, Canadian businesses are seeing more regulatory requirements in this area, including those related to breach reporting.

On November 1, 2018, amendments to PIPEDA came into force, creating a federal mandatory privacy breach reporting regime for Canada's private sector.

1 Catherine Beagan Flood and Nicole Henderson of Blakes represented one of the RESP defendants.

PIPEDA now requires an organization that experiences a "breach of security safeguards" involving personal information under the organization's control, where it is reasonable in the circumstances to believe that the breach poses a "real risk of significant harm" to affected individuals, to do the following:

1. Report the breach to the Privacy Commissioner of Canada
2. Notify affected individuals
3. Notify government institutions, parts of government institutions or other organizations if the organization believes that the institution (or part thereof) or other organization may be able to reduce or mitigate the risk of harm to the affected individuals.

PIPEDA also requires organizations to maintain a record of all breaches of security safeguards under the organization's control, even those that do not meet the harm threshold for reporting.

An organization that knowingly fails to report or maintain records of a breach as required by PIPEDA will be guilty of an offence punishable by fines of up to C$100,000.

PIPEDA's mandatory breach reporting regime adds to existing mandatory breach reporting regimes in Canada. For example, the Alberta *Personal Information Protection Act* has had mandatory breach reporting requirements since 2010, and many provincial health information statutes, which apply in the health-care sector, include mandatory breach reporting provisions.

On January 24, 2019, the Office of the Superintendent of Financial Institutions (OSFI) published the *Technology and Cyber Security Incident Reporting Advisory* (Advisory) applicable to all federally regulated financial institutions (FRFIs).

The Advisory, which comes into effect on March 31, 2019, requires FRFIs to report technology or cybersecurity incidents to OSFI where the incident is assessed as having a "high or critical severity level", such as where the incident is likely to result in extended disruptions to critical business systems or operations or have a material impact to critical deadlines or obligations in financial market settlement or payment systems.

It is important to note that the obligations under the Advisory apply regardless of whether the incident involved personal information and are therefore potentially broader than the mandatory notification and recordkeeping requirements under PIPEDA.

Regulators in other sectors have also issued guidance on cybersecurity, including the Canadian Securities Administrators, the Investment Industry Regulatory Organization of Canada, the Mutual Fund Dealers Association of Canada and, more recently, Health Canada with respect to medical devices.

As industries become more driven by and dependent on data, we can expect to see more regulatory requirements in this space.

4

Board Liability

While preventing all data breaches is a laudable objective, given the complexity of information systems and the ever-evolving ingenuity employed by cyber-attackers, such a goal may be impractical, and it is not the standard to which directors of Canadian companies should expect to be held accountable.

Consistent with their duty of care, boards of Canadian companies should practise prudent cybersecurity risk oversight fundamentals and continuously reassess the changing landscape of standards and risk.

The level of effort invested in privacy prevention should reflect the significance of the risk of breach and the potential harm to individuals. Developing a prevention strategy includes the following:

Privacy Management Structure: Ensure that a privacy officer, information security personnel and an incident response team are in place and review existing incident response plans, policies and procedures to identify any cybersecurity and data breach issues.

Data Mapping: Review the types of personal information collected by the organization and other critical data and ensure that data management practices are appropriate.

Assessment of Information Systems: Review the security tools in the organization's network and the software applications in place.

Preparation of an Incident Response Plan: Ensure that the organization has a plan that deals with breaches that compromise the personal information of clients or employees or the data of the organization, which includes the following tasks:

i. Implement an incident response team

ii. Define specific incident response procedures based on the category and severity of IT incident

iii. Define channels to report IT incidents

iv. Establish methods to track IT incidents through their lifecycle.

Training: Ensure that the organization's key information technology and information security personnel is properly trained on incident response and management.

Tabletop Exercise and Red Team Attacks: Conduct regular tabletop exercises and red team attacks with the organization's incident response team and other professionals.

Breach Coach: Retain an external legal counsel to serve as a breach coach.

Risk from Third-Party Relationships: Understand how the organization identifies, manages and assesses security risks posed by third-party products and services that it uses. To do so, the organization must evaluate the cyber-hygiene of its suppliers and mitigate risk and allocate liability through legal agreements with its suppliers.

CONTACTS

VANCOUVER

Eleni Kassaris
Partner
eleni.kassaris@blakes.com
604-631-3327

Alexandra Luchenko
Partner
alexandra.luchenko@blakes.com
604-631-4166

MONTRÉAL

Hélène Deschamps Marquis
Partner
helene.deschampsmarquis@blakes.com
514-982-4042

Sunny Handa
Partner
sunny.handa@blakes.com
514-982-4008

CALGARY

Birch Miller
Partner
birch.miller@blakes.com
403-260-9613

Darren Reed
Partner
darren.reed@blakes.com
403-260-9640

TORONTO

Imran Ahmad
Partner
imran.ahmad@blakes.com
416-863-4329

Catherine Beagan Flood
Partner
cbe@blakes.com
416-863-2269

David Feldman
Partner
david.feldman@blakes.com
416-863-4021

Iris Fischer
Partner
iris.fischer@blakes.com
416-863-2408

Nicole Henderson
Partner
nicole.henderson@blakes.com
416-863-2399

Wendy Mee
Partner
wendy.mee@blakes.com
416-863-3161