The Internet of Things and the Future of Risk

David Mackenzie
416-593-1221
dmackenzie@blaney.com

Rapidly Changing World of Risk

Fewer car accidents, and fewer injuries;

Retail Economy is moving online - may mean less commercial oriented personal injury;

buying online, and delivered to door.

Goods and Products are increasingly electronic and web-connected;

Businesses are web-facing, and collectors of sensitive information – face changing privacy and crime risk - - WannaCry?

Insurance is shifting to accommodate changing risk.

Blaney's Cyber Risk Work Today

With respect to cyber-risk, we represent insurers facing data breach and computer crime/social engineering claims.

We assist insurers navigating the 1st and 3rd party coverage they have issued (Cyber, CGL, E&O) when data breaches, privacy claims, or crime/ransomware claims are made by their policyholders.

We represent both the insurer in respect of coverage, and the policyholder with respect to defence of technology claims.

We assist in developing policy wording.

Blaneys' Cyber Experience

- We have represented many of the carriers here with respect to:
  - Coverage for hacking events;
  - Coverage for ransomware attacks;
  - Coverage for loss of control of PII;
  - Coverage for social engineering and computer fraud;
  - Coverage and defence of privacy torts;
  - Coverage and defence of technology errors & omissions claims.

What Will the Big Changes Be in 2,3,4,5 Years?

No one knows, but we can guess:

Fewer Car Accidents;
Less Personal Injury;

More privacy litigation
- mandatory breach reporting;

More technology litigation
- Every Product is a technology product

More regulatory litigation
- CASL / Data Use and Security Laws

Why Do We Say This?

- Internet of Things / Internet of Everything is Quickly Developing
  - Internet of Things: the ability of one device to connect to others through wireless infrastructure;
  - Internet of Everything – consumer products that wirelessly connect people with devices and the internet.
  - Unbelievable amount of data will be generated

Blaney McMurtry LLP

Development of the IoT/IoE

- There has been a lot of hype surrounding IoT/IoE. In many respects the hype has not yet been warranted.
- While we can buy “smart” washing machines and dishwashers, few people have.
- But, think of the devices in your home now that are connected: phones, computers, T.V.’s, speakers, smart meters, security cameras …

Development of the IoT/IoE

- Conservative estimates suggest 20 billion connected devices world-wide within 2 ½ years.
- IoT/IoE has been somewhat held back by inability to transmit all the data that can be generated.
- 5G is expected by 2020; 4G technology is being optimized for IoT/IoE.
- Connected Homes - Alexa/Amazon Echo/ Google Home – tip of the iceberg.

Development of IoT/IoE

Virtually, every product in the home, car, and office will be connected – you can buy “smart toothbrushes”!

Wearable technology is increasing in effectiveness and coming down in cost – all connected through smart phones;

Medical devices are increasingly connected;

Personal information about our location, health, habits and lifestyle, interests and vices, both inside and outside our homes will be available.

No longer able to “curate” our digital persona through Facebook / Instagram / LinkedIn and other social media. Our digital presence will be out of our control

How Will IoT/IoE Be Used By Policyholders

Good data is extraordinarily valuable. Microsoft paid US$26 Billion for LinkedIn. Microsoft could easily have written LinkedIn code itself, but paid for the data.

Data brokers buy data from data generators (IoT/IoE, smart phone apps, credit cards, loyalty cards et cetera) in order to generate accurate personal profiles.

These profiles are very specific to you. Sophisticated programs can easily identify individuals with little information. Your profile is bought and sold.

Allows businesses with the information to ensure that their marketing, services and products are specifically tailored to individuals.

Legal/Ethical Problems with Data Collection

- The information collected may be very personal or sensitive – family status, employment, financial information, health/mental health status, ethnic background, sexual orientation, immigration status…

- The information may include your image, allowing you to be identified electronically. As an article in the Atlantic Monthly said earlier this month: “You can’t encrypt your face”.

Legal/Ethical Problems with Data Collection

Unlike carefully monitoring what you place on social media, it is presently very difficult to control the information collected through IoT/IoE devices, except by not using them.

Consumers are often required to agree to Terms of Service/Clickwrap, but few read or understand them. They present a binary choice: use the product and give up your private information, or forego use of the product all together.

Consumers are giving away their rights to maintain private information, frequently without full awareness of the access to their smartphones/system they are providing and the nature and extent of the information that is being collected.

Legal/Ethical Problems with Data Collection

Given this lack of understanding, it is likely that once consumers do understand what they (unwittingly) have agreed to provide, they will become litigious.

Who will tell them about what they have agreed to? Plaintiff's class action counsel, of course! (remember, fewer car accidents and slip and falls?)

Legal/Ethical Problems with Data Collection

Class actions have already been commenced in the U.S. arising out of IoT/IoE. Bose headphones is facing class litigation:

> "Unbeknownst to its customers, however, Defendant designed Bose Connect to (i) collect and record the titles of the music and audio files its customers choose to play through their Bose wireless products and (ii) transmit such data along with other personal identifiers to third-parties—including a data miner—without its customers' knowledge or consent."

Legal/Ethical Problems with Data Collection

Who may use information collected, and how may they use it?

Should businesses be able to obtain PII and other confidential information to profile us for their commercial benefit? Amazon now has the ability to differentiate shoppers, and can price items differently based on profile and shopping history.

Who else can use such information, and for what? For example, should Landlords be able to obtain personal profiles from data collectors in order to assess “suitability”?

Regulation and class actions are likely to follow

Security - Who Is Protecting the Data?

IoT/IoE functions through the device passing information through a Wi-Fi network, sometimes onto to a smartphone, then to the cloud, which then passes it onto other servers for storage and analysis. The data may then be sold to others.

There is risk of criminal access or accidental loss at each stage of transmission. Like all other computers, security is only as strong as the weakest link in the chain.

As we have seen in the past week with Wannacry, computer security is uncertain at best. Every Windows user had 8 weeks to patch their systems. Every one of the victims (and their cyber-security people) had not done so. The state of your insured's cyber security is material to just about every risk you write now.

Blaney McMurtry LLP

Security - Who Is Protecting the Data?

IoT/IoE security is notoriously weak. Fall 2016 DDOS attack: Mirai virus accessed tens of thousands of IoT devices using passwords set by manufacturers and never changed. Attack shut down a number of websites for extended periods of time.

We are all interconnected online. The reason Wannacry was so successful is that it coupled malware with a worm. It was able to not only lock down individual computers, but also accessed others through network file sharing. Once a computer was infected, it could spread it to every other computer it could share a file with.

Malware is a huge problem. In 2014, 1 in 244 emails contained a threat, bot or malware. Last year that number rose to 1 in 131 (Symantec). Malware targets much more than email systems.

How is the Law Developing Now?

Common law is developing slowly.

Ontario courts have only just recently acknowledged common law privacy rights at all.

The common law privacy rights are narrow, and do not reflect the increasing importance of personal data.

The torts require proof of intent to harm. Unintentional loss of information to a hacker is not sufficient to prove loss under these torts.

Plaintiffs counsel are having to stretch the bounds of the torts to achieve recovery

How is the Law Developing Now?

Negligence is not proving to be a good angle for plaintiffs who have suffered privacy breaches.

Proof of actual injury is required in negligence.

The Home Depot class action demonstrates this difficulty. Home Depot lost credit and debit information of more than 500,000 people.

No one who had lost credit and debit information could prove a loss because banks bore the losses.

Class action settlement: $400,000.

However, lawsuits by banks against breached businesses are likely.

How is the Law Developing Now? - Breach

Emerging theories of liability for data breach.

Contract: Clickwrap and terms of service = contracts between consumer and service provider/retailer.

Such contracts include an implied term that the service provider/retailer will keep data provided by the consumer safe.

Failure to keep the data safe = breach of contract.

Breach of contract = damages.

How is the Law Developing Now? – Misuse of Data

Clickwrap and terms of service are being described as contracts by plaintiffs counsel.

If a business uses information in a manner that is not consistent with the clickwrap/terms of service, have they breached a contract with their customers?

LinkedIn faced liability for this when it scraped addresses from users email accounts, and sent “invite” emails to contacts.

Bose class action is premised on allegation that Bose did not obtain permission through its terms of service, such that it could sell user data.

Blaney McMurtry LLP

Likely Future Legal Developments?

Common law will likely struggle to keep up, so expect more regulation:

- Consumer protection legislation will likely be required to provide minimum terms under which entities may collect personal and confidential data.
- Such regulations may limit the use to which such data may be put, and regulate the manner in which data may be sold to third parties.
- Regulation will likely set minimum data security standards, and may provide safe harbors for those who comply.

Blaney McMurtry LLP

Likely Future Legal Developments?

- Developments in product liability laws to reflect electronic risks should be expected.
- Will IoT/IoE producers be held liable if:
  - Their products are hacked and data, personal information or other confidential information is lost due to inadequate security;
  - Their products transmit malware due to inadequate security;
  - Their products are actually used as part of a DDOS attack; or
  - Their products fail to satisfy a common understanding of “secure”?

What Does This Mean for Insurers?

As stated at the outset: The world of risk is changing. Policyholders will be looking for coverage for many of the risks outlined here.

The core insurance coverage for many businesses will likely be a combination of cyber/information policies and Technology Errors & Omissions policies.

The insurance industry will have to find a way to properly value data, so that its loss may be fully insured. This is not simply a matter of valuing a total loss of data, but also the loss of the exclusive use of data.

Insurers will be writing policies for a very uncertain world of risk, and will need to write “tight” wording, and set premiums accordingly, or face a new “asbestos” risk.

What Does This Mean for Insurers?

Coverage will still be found in legacy forms.

Many insurers have not updated the language of the CGL, bricks and mortar Property, Professional E&O and other policies to exclude or eliminate coverage also being sold (and priced) in cyber and technology forms.

Policies need to be patched the same way computers do. In a world of uncertain risk and uncertain law, the specific words used in policies will become even more critical.

What Does This Mean for Insurers?

Case in point : IBC CGL Personal and Advertising Injury form insures against:

> Oral or written publication, in any manner, of material that violates a person's right of privacy.

Three exclusions:

1. loss arising out of breach of contract;
2. Insureds in "Media and Internet type businesses;
3. loss arising out of an electronic bulletin board or chatroom

Consider the Bose Class Action – covered?