dri™ The Voice of the Defense Bar

Data and Security Dispatch

The newsletter of the
Cybersecurity and Data Privacy Committee

12/27/2018 Volume 4, Issue 3

Committee Leadership

Chair
Alexander E. Potente
Clyde & Co US LLP
San Francisco, CA

Immediate Past Chair
James H. Kallianis, Jr.
Hinshaw & Culbertson LLP
Chicago, Ill

Publications Chair/Newsletter Editors

Heyward Dodkin Bonyata
Nelson Mullins Riley & Scarborough
Columbia, SC

Wendy B. Degerman
Nelson Mullins Riley & Scarborough
Columbia, SC

Click here to view entire Leadership

In This Issue

Leadership Note

From the Chair

By Alex Potente

We have two exciting reads in this issue of the newsletter. First, Robert J. Cosgrove addresses the intersection between general liability and cyber coverages for consumer recalls from cyberattacks. Robert explains the limited nature of the coverages that appear under both, as well as the risks of your car sudden turning off while moving, driving a Porsche in London, and how to avoid Vogon-like confusion regarding cyber insurance products. Just ask Arthur Dent.

Second, Brent J. Arnold provides a year in review of Canadian cyber-insurance law. Brent addresses the formation of the Canadian Centre for Cyber Security, which combines formerly disparate government cyber security operational units, as well as the creation of an information-sharing pact under the Canadian Cyber Threat Exchange, Canada's first private sector hub for cyber security threat information sharing and analysis. The Threat Exchange enables the sharing of government-gathered threat intelligence, combining this intelligence with information gathered by member organizations. Brent also explains Canada's new cyber security strategy, which emphasizes security and resilience cyber innovation and leadership and collaboration, calls for additional action by the Canadian executive branch, and new mandatory breach reporting requirements under the Personal Information Protection and Electronic Documents Act.

I expect that you will find both of these articles as timely and informative as I have.

Alexander E. (Alex) Potente is a partner of Clyde & Co US LLP in Cleveland. He is an experienced trial lawyer who represents insurers in complex commercial insurance litigation matters including disputes pertaining to general liability and professional liability policies, with an emphasis on bad faith litigation and coverage issues arising from claims involving class actions, product defects, public sector liability and environmental and other long-tail insurance coverage disputes. He served as a law clerk for the Honorable James B. Zagel of the US District Court for the Northern District of Illinois from 1997 to 1999. Alex currently is chair of DRI's Cybersecurity and Data Privacy Committee.

Feature Articles

Porsches in London: Software, Cars and Recalls

By Robert J. Cosgrove

"There is a theory which states that if ever anyone discovers exactly what the Universe is for and why it is here, it will instantly disappear and be replaced by something even more bizarre and inexplicable. There is another theory which states that this has already happened."

The Official Hitchhiker's Guide to the Galaxy

After Earth's destruction, to make way for an intergalactic highway bypass, Arthur Dent, stumbles from planet to planet seeking to make sense of all the bizarre and inexplicable new experiences that surround him. If Arthur were to be dropped into the insurance galaxy of today, he would be similarly confused by the bizarre and inexplicable nature of the insurance products that exist that are all trying to fill the gap caused by the information world that we live in.

What do we mean? Well here's an example. I have a family of four young children and consequently we drive a SUV. The family SUV recently had to go into the shop for a routine inspection, oil change, tire rotation, etc. When the SUV was picked up, the invoice referenced a recall notification that had been remedied at the inspection. The mechanic was asked "what was the recall?" He responded—"Nothing serious. Just a software glitch with the satellite radio that

could cause the SUV's computer (which is connected to the satellite radio and which controls various car functions) to turn off without warning. You wouldn't believe how many calls we got when that glitch first hit!" Regardless of whether our mechanic was intentionally engaged in English style understatement— "WHAT!" A modern car, which is almost always run by a computer, simply shouldn't turn off. And software glitches which are not a physical part of the car do cause expensive recalls. And sometimes the software "glitches" are not glitches at all, but rather a cyber attack. And occasionally, software issues can cause fatal and other accidents.

Of course, where there are accidents and recalls, insurers and lawyers are sure to follow—even if the case law remains in its infancy. In the software glitch, auto accident scenario three types of "insurance" costs come up: (a) the cost of the recall; (b) the cost of the attack (and any resulting stolen data); and (c) money to pay for the property damage and bodily injury claims that inevitably result. But no one insurance product does all of these things and US courts have historically narrowly construed the coverage afforded by product recall, cyber, and commercial general liability policies. How so? Here's what the policies currently do.

Cyber policies typically provide two types of coverage: (a) first-party coverage for dealing with the costs of the recall; and (b) third-party coverage for the inevitable lawsuits. The Policy wording typically states that the insurer will defend (if applicable) or indemnify the insured for losses arising out of: a loss of digital assets, business interruption resulting from a computer system failure, cyber extortion, security event costs, and network security or privacy breaches. The wording is bespoke and the coverage is claims made. But, regardless of the specifics, these policies focus on protecting and responding to information, not physical things. Cars are, for the moment, very physical things and so cyber policies aren't really on point.

What then of recall policies? Well, the traditional recall policy is meant to respond to the recall, withdrawal, repair or replacement of "Insured Product." It is also a claims made, indemnity policy that does not provide the insured with a defense from lawsuits. Coverage only attaches if the affected product has caused or would cause "bodily injury" or "property damage," or was ordered to be recalled by a government agency. Notably, recall policies often contain exclusions for the failure of computers or software if those failures were the cause of the recall. So, in our car context, a recall policy is unlikely to indemnify the car manufacturer for a software glitch and it certainly is not going to provide a defense if the car manufacturer is sued when that software glitch causes a fatal crash.

Then, of course, we have commercial general liability policies that insure "occurrences," a/k/a accidents or fortuitous losses. The policies provide a defense for damages for which the insured is liable because of "bodily injury," "property damage" or "personal and advertising injury." What they're not meant to insure is business risks—which, of course, is why the policies contain damages to your product, damage to your work and recall of products exclusions. What one often sees are attempts to convert CGL policies into craftsmanship guarantor policies—just ask any construction defect litigator. This is usually done, with a nod and a wink, by pretending that the case isn't really about the defective workmanship or the "bad" product, but rather the consequential damages that flow from that work or bad product. In other words (as an example only – we're not trying to create new theories of innovation for plaintiffs' attorneys), we're not seeking coverage for the fact that we had to fix all these broken cars, we're seeking coverage for the fact that the broken cars damaged their owners' ability to make money! In general, these novel claims are disfavored by the courts (at least in the Northeast).

Which leads us then to the question of solutions since for every problem, there's an opportunity. What does all of this mean for lawyers and the courts?

First, we anticipate that policyholders' counsel will continue to aggressively attempt to convert commercial general liability policies into the Swiss Army knives of insurance coverage. Most likely these attempts will focus less on claiming that software issues caused "property damage," but rather that they qualify as "personal and advertising injury" such that a duty to defend exists—much like what the trial court (later affirmed by the Fourth Circuit in an unpublished decision) did in the case of *Travelers Indem. v. Portal Healthcare*, 35 F. Supp. 3d 765 (EDVA 2014). Triggering a duty to defend is the low hanging fruit as defenses get expensive and indemnity coverage decisions can be difficult to achieve until the underlying case is resolved.

Second, we anticipate that the insurance markets will begin to wrap their product recall policies with cyber coverage on top. Specifically, we anticipate that the product recall policies will affirmatively begin to cover computer and software related claims. Insurers are much like lemmings and where one goes, others follow.

Third, we anticipate that cyber coverage will continue to evolve from "data" or "information" based to also providing coverage for physical things. Some insurance companies

have already created products to do exactly that. But these policies remain expensive and thus cater to the "high end" of the insurance market. As momentum picks up, the cost of these "wrap" policies will decrease and your corner bodega will start to have cyber cover written on top of base property and casualty coverage.

But, you might ask, what does all of this mean for you? For the moment, the "cyber" world is the province of the AmLaw 100 and has focused on the largest insureds and the biggest claims. We anticipate that this will begin to change within 3 to 5 years. Once it does: (a) defense attorneys will need to know to ask for more than the declarations page of a CGL policy as part of discovery; (b) coverage attorneys will have to examine an ever expanding universe of potential coverages to determine whether coverage attaches under a particular policy, and, if it does, how does it "stack" relevant to other policies; and (c) there will be a multitude of new subrogation/contribution opportunities, that will require practitioners to bulk up their understanding of the digital world and how to press claims in it.

"Driving a Porsche in London is like bringing a Ming vase to a football game."

- The Official Hitchhiker's Guide to the Galaxy

Jumping back to good old Arthur, safe from the Vogons, he was able, thanks to the dolphins (please don't ask), to find order out of the chaos that had enveloped him, through a rebuilt Earth. There are many opportunities to do exactly this in the legal world today. But there are dangers we need to avoid—sort of like how one acts when trying to prevent damage while driving a Porsche in London.

Bob Cosgrove, a CIPP – US, CIPM is a partner at Wade Clark Mulcahy – wcmlaw.com, a regional defense firm with offices in NY, NJ and PA. A former prosecutor, Cosgrove is a graduate of Georgetown University's School of Foreign Service and Fordham University's School of Law.

2018: The Year (So Far) in Review in Canadian Cyber Security

By Brent J. Arnold

With a few weeks to go, 2018 has already seen a number of important developments in Canadian cybersecurity and data privacy, including a complete overhaul of Canada's security establishment, calls for a new federal ministry to combat cyber threats, and the rollout of a more robust data privacy regime.

The Canadian Centre for Cyber Security

On October 1, just in time for Cyber Security Awareness month, Canada's Minister of National Defence announced the launch of the new Canadian Centre for Cyber Security ("CCCS"). Government of Canada Communications Security Establishment, "The Minister of National Defence Announces the Launch of the Canadian Centre for Cyber Security." The CCCS's homepage may be found here. First announced in June 2018, the creation of the CCCS brings together formerly disparate government cyber security operational units, and enhances the federal government's leadership role in cyber security.

CCCS assumes a broad portfolio of responsibilities, bringing under the umbrella of the Canadian Security Establishment ("CSE") many areas formerly housed under Public Safety Canada ("PSC"). The new CSE branch describes its role as follows:

- Informing Canada and Canadians about cyber security matters, as a single, clear, trusted source of information on cyber security for Canadians and businesses;
- Protecting Canadians' cyber security interests through targeted advice, specific guidance, direct hands-on assistance, and strong collaborative partnerships;
- Developing and sharing specialized cyber defense technologies and tools resulting in better cyber security for all Canadians;
- Defending cyber systems, including government systems, by deploying sophisticated cyber defense solutions ;
- Acting as the operational leader and government spokesperson during cyber security events.

Id.

The reorganization installs CCCS as the primary government portal for Canadians seeking information on cyber security, identity theft, and related issues. Both the Canadian Cyber Incident Response Centre ("CCIRC") and the PSC's "Get Cyber Safe" public information campaign are now in CCCS's bailiwick. The newly launched CCCS website features an updated Get Cyber Safe campaign page with a wealth of information on everything from identity theft to protecting small businesses to cyberbullying to current online scams and frauds, and users can also interact with the Get Cyber Safe campaign across a number of social media platforms. These include Twitter, Facebook, Instagram, and for the small or medium business owner, LinkedIn.

Apart from providing resources to the public, CCCS intends to assert the government's leadership role in cyber security by collaborating with owners of critical infrastructure, other levels of government within Canada's federal system, and industry. It will work with cyber security vendors in the development of products, play the role of technical authority, and offer downloadable tools such as its open-source "Assemblyline" malware detection and analysis software, originally released in late 2017. Assemblyline is now available here.

CCCS is deepening the government's collaboration with industry by entering into an information-sharing pact with the Canadian Cyber Threat Exchange ("CCTX"), Canada's first private sector hub for cyber security threat information sharing and analysis. The pact, announced in September before the CCCS rollout and signed the same day CCCS went live, provides for the sharing of government-gathered threat intelligence, combining this intelligence with information gathered by CCTX member organizations (which include key players in Canadian critical infrastructure sectors such as telecommunications, banking, and transportation).

Canada's New Cyber Security Strategy

The CCCS is just one part of the Government of Canada's new cyber security strategy, released in June 2018 and backed with a commitment in the 2018 federal budget of $507.7 million in funding over five years. *See* Government of Canada Public Safety Canada, National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age; Alex Boutilier, *The Toronto Star*, "Liberals pitch $500 million cyber security plan."

Canada's last national cyber security strategy was launched in 2010, when large-scale cyber attacks were less common and aggressive cyber activity by state actors was little heard of. Canada was, arguably, long overdue for a review of its cyber security posture. Recognizing this, the federal government commissioned a comprehensive review of the 2010 cyber security strategy in 2016, culminating in a report released in 2017 that identified, among other issues, the need for greater public awareness and for greater public funding and resources in the field of cyber security. Nielsen, Cyber Review Consultations Report. The new strategy is built on three themes:

- Security and resilience (by maintaining and improving the cyber security posture of federal departments and agencies, and enhancing law enforcement's ability to investigate and respond to cybercrime);
- Cyber innovation (including driving investment and research and development in cyber security, focusing on "emerging areas of Canadian excellence" including quantum computing and blockchain); and
- Leadership and collaboration (by establishing "a clear focal point for authoritative advice, guidance, and cyber incident response," "reinvigorat[ing] public awareness and engagement efforts and establish[ing] new forums for collaboration," and partnering with the provinces to develop a "national plan to prevent, mitigate and respond to cyber incidents").

National Cyber Security Strategy, *supra,* at p.17, 24, 31.

Unlike its more granular 2010 predecessor, the 2018 strategy is aspirational and short on specifics by design; it is intended to provide a flexible theoretical framework for the more concrete measures to be set out in action plans to come. The CCCS, along with the creation of an RCMP National Cybercrime Coordination Unit, is among the first tangible examples of Canada's renewed commitment to cyber security. *Id.* at p.iii.

A Senate Committee Report Calls for Sweeping Changes to Canadian Cyber Security

Just a few months after the federal government rolled out this new strategy, the legislature weighed in with calls for still more concrete action from the executive branch. On October 29, the Canadian Senate's Standing Committee on Banking, Trade and Commerce released a brief-but-alarming report titled *Cyber.assault: It should keep you up at night*. Senate Canada, Report of the Standing Senate Committee on Banking, Trade and Commerce, Cyber.assault: It should keep you up at night (Ottawa: October 29, 2018). The report highlights Canadians' increasing exposure to cyber threats and notes that, despite a year of government progress,

"there is much more that the federal government and Canadians must do to protect ourselves. We must take the appropriate steps now, or soon we will all be victims." *Id.* at p.8. The report recommends sweeping changes and the allocation of more federal resources. Among the Committee's recommendations are:

- Federal government funding for:
  - cyber security skills training programs, in collaboration with the provinces, territories, and municipalities, to assist businesses with their cyber security needs;
  - Three national centres of excellence in cyber security research in order to promote basic research in the science of cyber security and to encourage Canadians to pursue education and careers in cyber security-related fields;
  - A national cyber literacy program, led by the CCCS;
- A federal rapid and responsive national cyber security information sharing framework and changes to federal privacy legislation to allow information sharing about cyber threats within the private sector and between the private sector, government, and relevant international organizations;
- Tax incentives for all businesses, particularly those in critical infrastructure sectors, to improve their cyber security practices;
- Modernization of federal privacy legislation and the vesting of the federal Office of the Privacy Commissioner with the power to make orders and impose fines against companies that have failed to take adequate measures to protect customers' personal information;
- The creation of a new federal minister of cyber security responsible for cyber security policy, including the national cyber security strategy, who would have oversight over the CCCS and the National Cybercrime Coordination Unit.

See id. Senate Canada, Report of the Standing Senate Committee on Banking, Trade and Commerce, Cyber. assault: It should keep you up at night (Ottawa: October 29, 2018) at pp.6–10.

The federal government's position on these suggested reforms is not yet known, although at least some of the recommendations (such as the public education campaign and increased public-private threat information sharing) have already been taken up by the CCCS as part of its new mandate.

Mandatory Breach Reporting Comes to Canada

Starting November 1, private sector organizations subject to the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*")—and this includes most organizations, as it applies except in those few provinces with their own legislation governing the commercial collection of personal information—will be subject to mandatory breach notification requirements. Reporting will be required in circumstances where it is reasonable to believe that the breach creates a "real risk of significant harm to the individual." Such harm may include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property. For more information, see Joshua Shoemaker, Wendy Wagner, and Naïm Alexandre Antaki," IPEDA Data Breach Reporting to Take Effect November 1, 2018.

Conclusion

2018 has seen a number of important if belated improvements in Canada's cyber security posture. It will be fascinating to see how quickly and to what degree these changes bring about measurable results.

Brent J. Arnold is a partner practicing in Gowling WLG's advocacy department in Toronto, specializing in commercial litigation and arbitration. Brent heads the firm's Commercial Litigation Technology Sub-group. He also leads cybersecurity initiatives for the firm's Financial Services Regulatory Group, and is a member of its Insurtech Group and its Innovation Council. Brent's experience includes cyber breach coaching, cyber risk, and consumer, implementation, and other disputes for e-commerce vendors and software developers. He also has experience in construction, franchise, administrative, and insolvency law, shareholders' rights, class actions, employment contracts, intellectual property-related disputes in the Superior Court of Justice, and general contractual disputes. He has appeared before all levels of court in Ontario, including the Court of Appeal and the Supreme Court of Canada, and has appeared before the Licence Appeal Tribunal, the Human Rights Tribunal of Ontario, the OMVIC Discipline and Appeals Committee, and the Ontario Municipal Board. In 2011, Brent appeared before the Supreme Court of Canada in support of the federal government's constitutional reference regarding a Canadian Securities Act.