Blaney McMurtry LLP

PUBLICATION

Privacy Regulation and Emerging Risks for Insurers

Date: June 12, 2018
Co-Author: David Mackenzie

This article was originally published by Euromoney's Expert Guides: Best of the Best. Click here to view the PDF file.

Introduction

On April 9th 2018 87 million people around the globe were notified that the personal information contained on their Facebook profiles had been accessed without their consent. The data was accessed by Cambridge Analytica and allegedly had been used to influence the outcome of the American Presidential election. The data breach exposed a major loophole in Facebook's privacy policy which allows third party application developers to access data from the "friends" of the users of their application. Cambridge Analytica was able to harvest data from 87 million Facebook accounts even though fewer than 300,000 people used the application it designed. This is not the first major online breach of privacy, nor will it be the last.

People have increasingly lost their ability to determine and regulate their own individual zone of personal privacy. While most people expect to maintain some control over their personal information, that ability is quickly being lost to technological advancement. The implications of this fact are profound for liability insurers. As the electronic and digital world becomes more pervasive, individuals lose the ability to manage and control the personal information which is available to others. In an effort to limit technology's most intrusive effects, various legislative bodies are beginning to develop regulation to exert control over the manner in which personal information may be collected and used. These emerging issues go beyond privacy loss as the result of malicious or accidental data breach and concern the legality and ethics of what are, increasingly, everyday business practices. The conflict emerging between new, interconnected technology and legal restrictions will almost certainly result in litigation involving policyholders. This will, in turn, lead to insurance coverage litigation.

The Emergence of New Regulation

On May 25th 2018 the European General Data Protection Regulation ("GDPR") will come into full force and effect. The GDPR purports to govern any organization, anywhere in the world, if that organization collects or stores personal data relating to citizens of the European Union. Focusing on informed consent, the GDPR imposes onerous conditions on entities falling within its ambit and provides for sanctions up to the greater of €20 million or 4% of global turnover. The implications of the GDPR for North American organizations are, as of yet, uncertain. Nevertheless, they are probably difficult to overstate. The broadly drafted definition of "personal data" will leave many entities within its reach. Any entity with a significant digital presence will likely be exposed to substantial liability if its business incorporates the possession or processing of the personal data of European citizens.

The expansion of privacy regulation is occurring concurrently in Canada. New regulations are coming into force under the Federal Personal Information Protection and Electronic Documents Act ("PIPEDA") and under provincial legislation like Ontario's Personal Health Information Privacy Act ("PHIPA"). Both pieces of legislation have created new data breach reporting requirements. Importantly, changes to PIPEDA focus not only on breach reporting but also on how information may be collected and used. In common with the GDPR, PIPEDA focuses on consent of the individual to collection and specific use of personal information. These expanded privacy rights are also being re-enforced in the Courts. Canada's Supreme Court, for example, has recently ruled that the right to privacy is of a "quasi-constitutional" nature.

The global proliferation of privacy regulation is likely to pose acute challenges for a wide variety of businesses. The increased challenge and exposure to liability will inevitably lead to increased claims for insurance coverage under a wide variety of commercial insurance policies.

Issues for Liability Insurers

Expanding privacy based liability raises the possibility of both great risk and reward for insurers. As an emerging area of risk, there are considerable opportunities for insurers who undertake careful review of emerging trends and introduce appropriate products into the market. Presently, however, insurance against privacy risk exists in a climate of uncertainty. Coverage for privacy risk is found in numerous forms of commercial insurance. The fact that coverage for privacy risk is present in such a wide variety of policies is indicative of the extent to which insurance providers have not yet fully assessed its implications.

Cyber Policies

Cyber insurance will virtually always cover malicious hacking events or inappropriate access by employees. Beyond that, however, given the lack of standard wording, nothing else is certain. Whether or not a cyber policy will cover violations of personal privacy rights can only be determined by a detailed review of the specific policy wording. Should an insured entity face a claim for improper use of personal data, an entitlement to coverage will depend on whether or not the insured bought sufficiently broad coverage. In general, cyber policies will provide both first and third party coverage. Even in circumstances wherein regulatory action or penalties and fines are in issue, first party obligations may still arise. For example, a cyber-policy could be

liable for the first party costs of removing data from an insured's systems if that data is in violation of privacy laws or regulations. This may be so even if coverage is unavailable for the insured's third party or regulatory exposure. As a result of the current regulatory uncertainties and the lack of standard coverage language, cyber policies are likely to be the subject of substantial coverage litigation.

Commercial General Liability

Privacy coverage remains available in standard from Commercial General Liability policies. Part B of these policies provides insurance against "oral or written publication, in any manner, of material that violates a person's right to privacy". Coverage questions with respect to data management practices by policyholders are already arising.

The meaning of the term "publication" has not been defined in standard CGL policies. Without such definition, the meaning of "publication" has become contentions, with insurers and policyholders turning to the courts for resolution. Important legal precedent with respect to the scope of the term "publication" in malicious and unintentional data breach events will become a question litigated with growing frequency. As personal privacy right claims advance, that trend should be expected to continue.

Errors and Omissions

Great reliance is placed on professionals throughout the entirety of the technology sector. With the added complexity generated by the growing restrictions on how information may be used, professional technical assistance will only grow more critical. Good coding will be of central importance to businesses that successfully navigate privacy risk. Many companies rely on automated algorithms for processes such as targeted advertisement generation and consumer recommendation functions. These companies often outsource their program and application development. If errors or deficiencies in the computer code result in a breach of privacy regulations, litigation will likely ensue against the coder. Such a claim will likely qualify as a "wrongful act" under an Errors & Omissions policy. In Canada many professional E&O policies already provide coverage for liability arising out of PIPEDA, however recent revisions to PIPEDA may cause carriers to reassess their willingness to underwrite this exposure.

Directors and Officers

The expansion of potential exposure arising out of personal data privacy claims provides additional challenges for Directors and Officers of business entities. For entities with an international presence, careful consideration will have to be given to the requirements of emerging privacy law in order to ensure that operations remain compliant. The GDPR requires that certain organizations have Data Protection Officers ("DPO"), who report directly to the board. Under GDPR rules, these DPO's cannot be fired for performing their statutory obligations.

Failure to comply with legal or regulatory obligations related to use and processing of personal data can expose organizations to very significant liability to damages or penalties and defense costs. Should an entity find themselves subject to such damages or penalties, litigation against board members would not be surprising. Policyholders facing potential risk with respect to

common law privacy torts or regulatory regimes like the GDPR will need to carefully consider adequacy of limits. While it seems unlikely that organizations will be exposed to maximum regulatory penalties, the possibility cannot be ignored. Underwriters should, therefore, include personal data privacy risk in their calculations.

Conclusion

The internet and electronic communications are not governed by borders. As a result, legislative regimes are seeking to impose regulations with transnational application. As privacy regulation develops to address modern technological issues, these factors are colliding to create new, emerging, commercial liability risks. Insurers will unquestionably be called upon to provide coverage for these new risks. While many of the new policy forms entering the market may address some or much of the emerging privacy risk, legacy forms will continue to be triggered. Coverage litigation is bound to proliferate. Those advising insurers and policyholders should be prepared.