Privacy class actions, by the numbers

- Christopher Naudie
- Evan Thomas

May 31, 2017

The past five years have seen an increased awareness of the risk of privacy class actions. This time period coincides with the recognition by various courts of the common law tort of intrusion upon seclusion (invasion of privacy) and an increasing incidence of privacy breaches arising from hacking, misuse of information by employees, theft or loss of personal information, and other causes.

Using a database of 59 privacy class actions maintained by Osler's AccessPrivacy, we have identified a number of trends in privacy class actions:

- Not surprisingly, the number of Canadian privacy class actions has increased significantly over the past five years.
- Hacking incidents account for nearly 1/3 of all privacy class actions, and the share of all privacy class actions represented by hacking incidents appears to be increasing over time.
- Misuse of information by employees and theft or loss of physical media containing personal information also account for a significant proportion of privacy class actions.
- Ontario is the jurisdiction of choice for plaintiffs bringing privacy class actions, though Quebec and British Columbia also have a large number of privacy class actions pending before their courts.
- Technology/media companies and health care providers are the organizations most frequently named in privacy class actions, which is perhaps not surprising in light of the volume and nature of the data such organizations collect and use on a day-to-day basis.

Privacy class actions over time

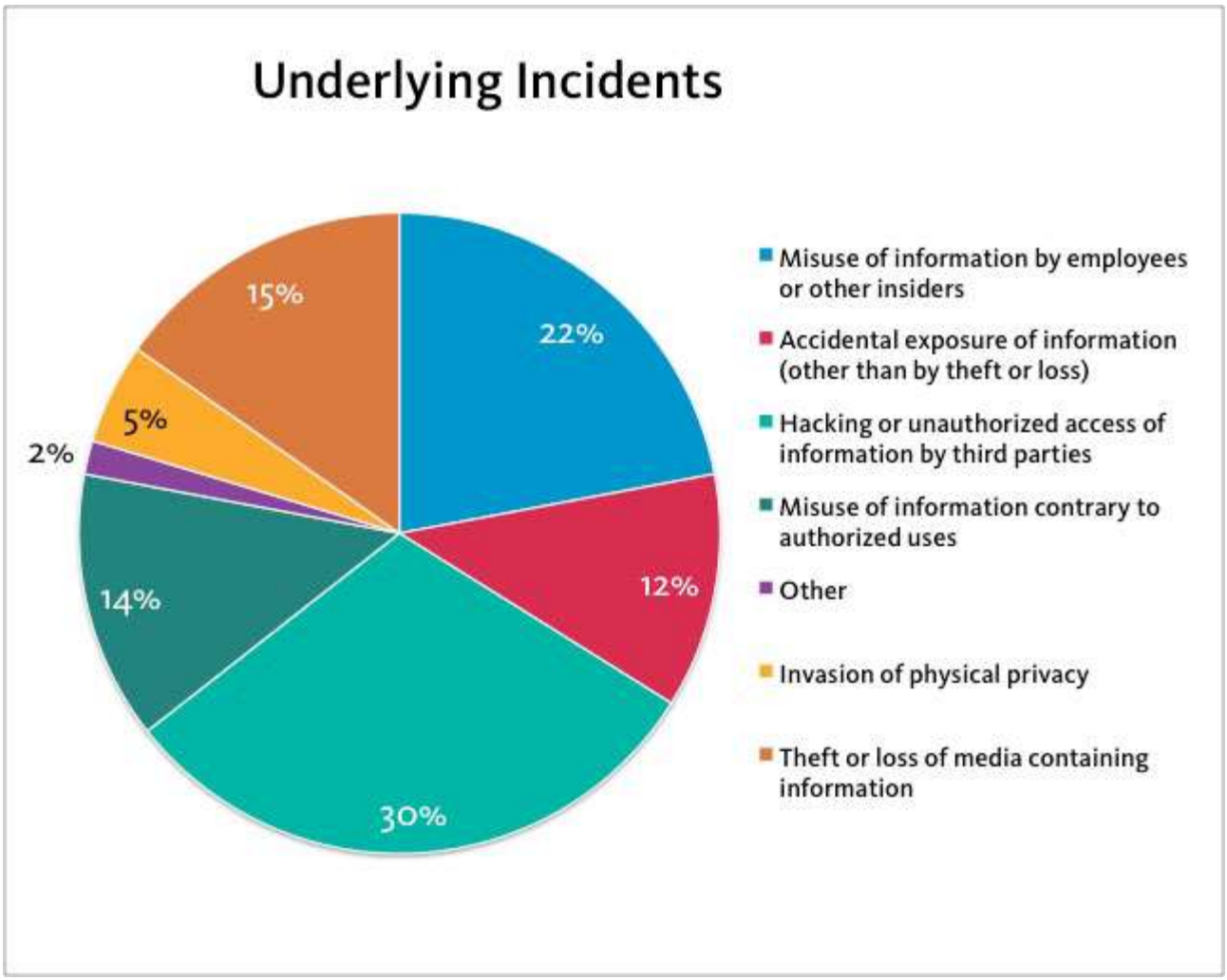
The number of privacy class actions rapidly increased from 2010 to 2016. There were only two privacy class actions commenced prior to 2010. 2010 saw three, new privacy class actions, rising to 7 in 2011 and 10 in each of 2012 and 2013. Following a slight dip in 2014 and 2015, there were 11 commenced in 2016. So far in 2017, we are aware of four new privacy class actions.

By underlying privacy incident

A variety of privacy incidents may result in a privacy class action: hacking of computer systems by outside actors, misuse of information by employees or other insiders with access to the information, theft or loss of physical media containing personal information, accidental exposure of personal information, invasions of physical privacy, and alleged misuse of information contrary to the purpose for which it was collected.

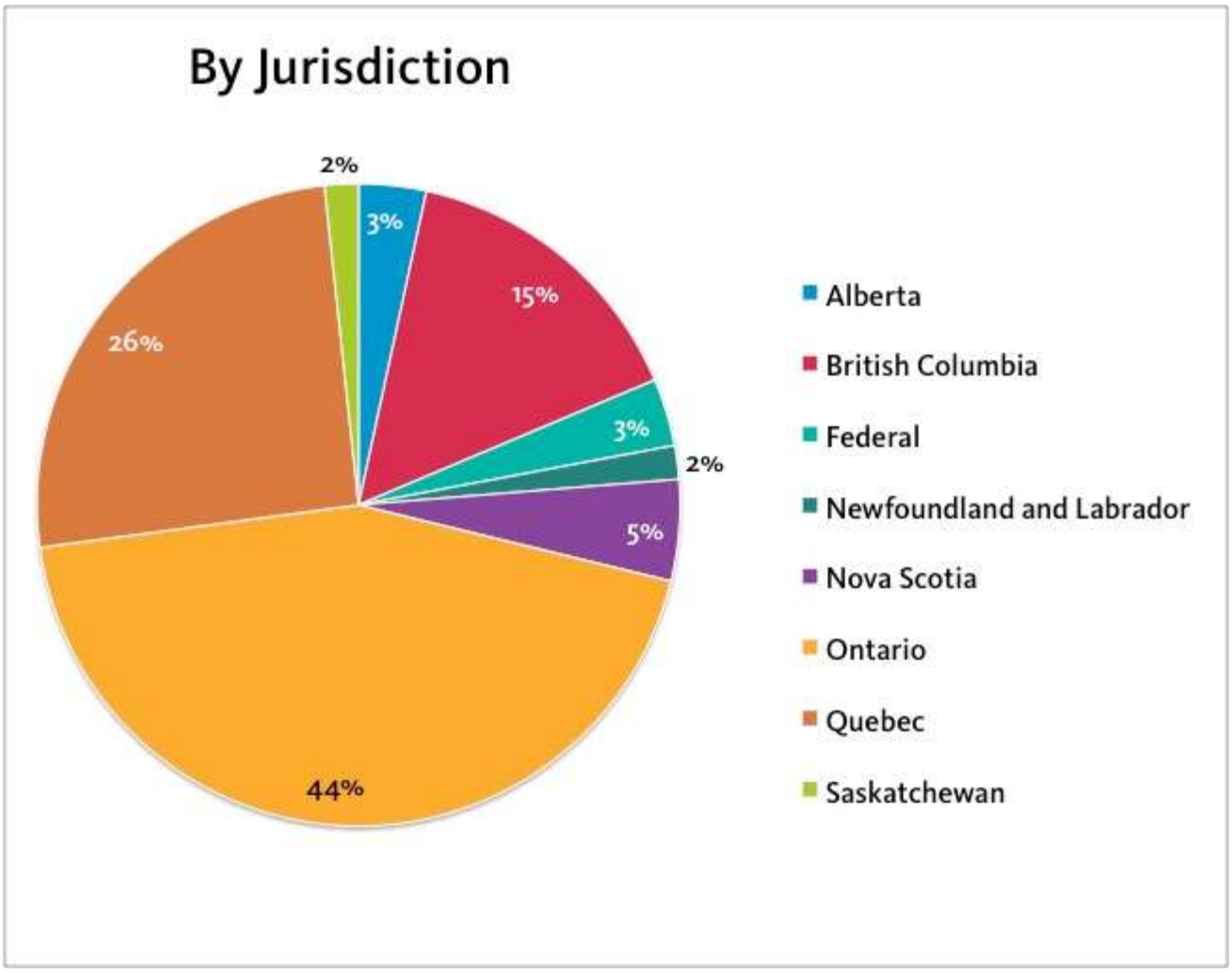
Hacking incidents are the leading cause of privacy class actions, accounting for 18, or approximately 1/3, of the privacy class actions in our database. Misuse of information by employees and other insiders accounts for 13 (around 20%) of privacy class actions, followed by incidents involving theft or loss of physical media, which account for 9, or about 15% of the total.

Interestingly, most hacking-related privacy class actions have been commenced since 2013, and so the share of privacy class actions represented by hacking incidents is increasing over time. On the other hand, privacy class actions arising from the loss, theft or other accidental exposure of personal information appear to be less frequent over time. This may reflect a growing awareness by organizations of the need to protect personal information using encryption and other data protection measures.



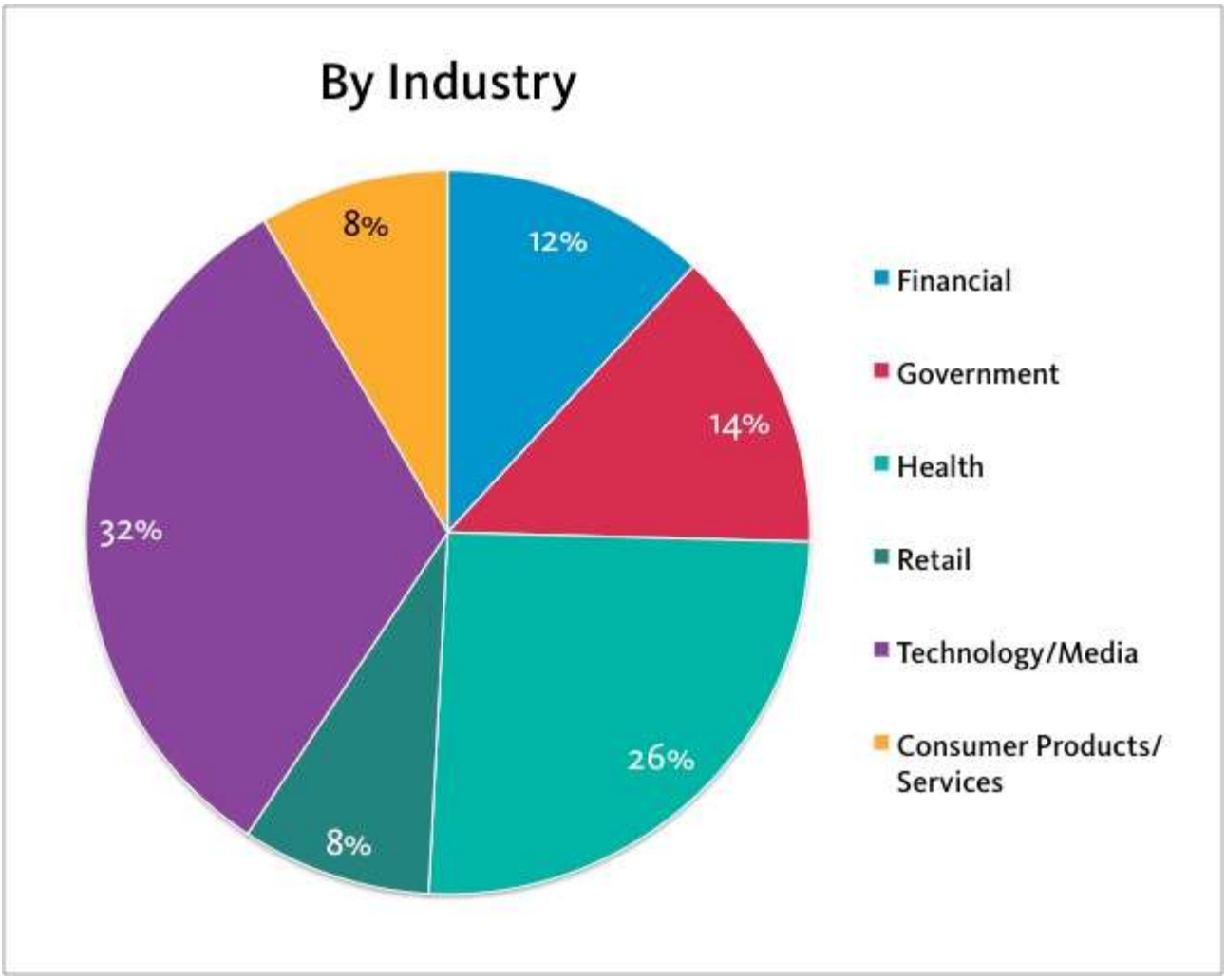
By jurisdiction

Ontario is the most popular jurisdiction for commencing privacy class actions. Nearly half (26 of 59) of privacy class actions have been commenced in Ontario.[1] Quebec and British Columbia account for 15 (25%) and 9 (15%), respectively.



By industry

Almost 1/3 of privacy class actions have been against technology or media companies. Another 25% or so have been against health care providers. Financial institutions and governments are also frequently named as defendants.



Conclusion

Despite the increase in the number of privacy class actions over the past five years, it appears that the number of class actions is still significantly less than the number of publicly disclosed privacy breaches. Hacking incidents account for a significant percentage of privacy class actions, and this is only increasing with time, but it would appear that only the largest and/or highest profile hacking incidents are resulting in class actions. This suggests that plaintiffs' counsel are selective in the number of privacy breach cases they will take on as potential class actions. Not surprisingly, privacy class actions are concentrated in Ontario, Quebec and British Columbia, which are the largest provinces by population and have well-established class action bars. As well, the most frequent targets of privacy class actions are technology/media companies and health care providers, consistent with the large volume of personal information usde in such organizations.

Osler has more details on these claims and trends available through Access Privacy.

[1] Where multiple class actions arising from the same incident are commenced in different jurisdictions, these are counted separately. Where multiple class actions arising from the same incident are commenced in one jurisdiction, they are counted as a single class action because we assume that the court will only permit one class action to proceed.