In the Internet of Things, Opportunities Abound for Class Action Litigation

July 20, 2018

At an estimated 8.4 billion in number, connected devices now in use outnumber people on earth.[1] It is estimated that the usage of these devices will continue to grow, reaching 20 billion devices over the next two years and 50 billion devices by 2050.[2] The Internet of Things (IoT) describes the milieu of these connected devices, which are connected to each other and to the internet. IoT technologies are transforming not only industrial processes but the way people do business. Their effect is far reaching, cutting across all disciplines and industries. These connected devices range from wearables, children's smart toys and home appliances, to digital health devices and autonomous vehicles.

In this new world of product development, IoT technologies are marked by shorter product and adoption cycles and have the capability to collect, store, and exchange highly specific data about their users. Product failures or vulnerabilities of IoT devices may not only lead to privacy breaches, but also to property damage, personal injury, and economic loss claims. Class actions may well become an effective litigation tool for advancing claims involving IoT technology failures. As recent IoT class action jurisprudence demonstrates, IoT product failures may be exposed by an ill-intentioned third party in the course of a cyber-attack or through benign schemes driven by research and journalistic initiatives.[3] At times, the exposed vulnerability may necessitate a product recall.[4]

Recent IoT class actions south of the border demonstrate the rich variety of claims being advanced by plaintiffs: privacy and warranty breaches, negligent design and manufacture, unjust enrichment, fraud and failure to warn claims. While there may be cases where defendants will agree to a settlement,[5]the current tendency has been for defendants to fight the merits of the claims being advanced. In the cases to-date, the defendants have prevailed where it has been demonstrated there was no evidence that any of the plaintiffs experienced the alleged product failure.

This strategy of resistance has not always reaped benefits for the challenging defendants. A recent example is the July 5, 2018 ruling in *Flynn v. FCA.* Despite there being no evidence that any of the plaintiffs' vehicles were hacked into as a result of the alleged cybersecurity flaws of their connected vehicles' infotainment system, a U.S. Federal Court declined to order summary judgment with respect to all of the plaintiffs' claims. The Court found there existed a genuine dispute as to whether the class vehicles had defects, whether the alleged defects were remedied by the recall and

whether additional measures were required to protect the vehicles from an unreasonable risk of hacking.[6] While the Court found that the plaintiffs' unjust enrichment claims lacked merit, the warranty claims survived the summary judgment motion, as did some of the plaintiffs' claims for fraudulent misrepresentation. Ultimately, the Court granted partial certification of three classes of plaintiffs in Michigan, Illinois, and Missouri. As this decision is expected to be appealed, it remains to be seen whose arguments will ultimately prevail.

Takeaways

What should IoT manufacturers, distributors, suppliers, and platform providers do in the face of this product litigation risk? The best practice may well be to exercise due diligence in ensuring the security integrity of the IoT device, both for the device itself as well as anything that connects to it. Particularly in cases where there is no evidence that any class member suffered the alleged product failure, it would appear that challenging the merits of the claim pre-certification may have some merit.[7]

In conclusion, while courts are still defining the parameters for IoT class actions, class actions are expected to be an attractive option for plaintiffs to seek recovery for losses incurred from IoT product failures. In this changing landscape, it will be important for IoT device manufacturers, distributors, suppliers, and platform providers to not only inoculate against security failures before the product hits the market but also to continue to conduct post-market product surveillance in order to deploy safety and security reinforcements during the product life cycle.

[1] Gartner, Press Release, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016" (7 February 2017), online: https://www.gartner.com/newsroom/id/3598917

[2] Leta Gortman, "The Era of the Internet of Things: Can Product Liability Laws Keep Up" 84 Def. Counsel J. 1 (2017) at p. 1-2.

[3] *Ross v St Jude Medical Inc,* No 2:16- cv- 06465 (CD Cal 2016); *Cahen v Toyota Motor Corp*, 14 F Supp 3d 955 (ND Cal 2015); and *Flynn v FCA US LLC*, 3:15-cv-00855 (SD III 2015).

[4] *Cahen v Toyota Motor Corp*, 14 F Supp 3d 955, 971 (ND Cal 2015).

[5] *NP and PS v Standard Innovation Corp*, No 1:16-cv-8655 (ND Ill 2017).

[6] *Flynn v FCA US LLC*, 3:15-cv-00855 (SD III 2015), see page of the July 2018 decision of Justice Reagan.

[7] See: *Lozanski v the Home Depot* 2016 ONSC 5447 at para 48 and 74. The alleged loss stemmed from a data breach of the Home Depot's payment card systems by a hacker using custom-built malware. Although this was a motion for approval of settlement, among other things, the court noted that it would have approved a discontinuance in part because there was no allegation on the part of any class member that he or she suffered a financial loss attributable to the data breach. The Court also noted that the company had fulfilled its obligations to respond to the hacking and to

notify its customers and had done so in a responsible, prompt, generous and exemplary fashion.

By

Glenn Zakaib, Edona C. Vila

Expertise

Class Action Defence, Banking Litigation, Cybersecurity, Privacy & Data Protection

---

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.