GlobalResearch
Center for Research on Globalization

Holding Uber Accountable: Litigating over Data Hacks

By Dr. Binoy Kampmark
Global Research, December 03, 2017
Region: USA
Theme: Intelligence, Law and Justice

It sent patrons and users into fits of puzzled anger. It numbed a good many more who had placed mistaken faith in its operations. Rapacious, predatory Uber, a ride-hailing company famed for its international ruthlessness, had behaved accordingly. Last week, the firm revealed that it had received a massive hack in 2016, failing to notify customers and regulators that a breach of security had taken place.

The scale of the hack was far from negligible. Some 57 million customers were affected, their data obtained and held to ransom. This was not all. Officials at Uber, having decided against immediate revelation in favour of a deep freeze approach, went for an eyebrow raising option: paying off the culprits to the tune of $100,000. A dark deal was done: pretend it had never happened. The hackers walked away delighted.

Given the nature of such information hacks, the hide and seek option was never going to last. In a blog post, the company subsequently conceded that, "In October 2016, Uber experienced a data security incident that resulted in a breach of information related to rider and driver accounts."

The data compromised involved names, email addresses and mobile phone numbers. Certain "forensic experts" were cited as claiming that no "trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded."

Incoming chief executive Dara Khosrowshahi apologised with predictable insincerity – when accepting the job in August, he already had knowledge of the hack. "None of this should have happened, and I will not make excuses for it."

Having been exposed for being in the breach, Uber's next step was to claim that the hacking was insipid. There had been "no evidence of fraud or misuse tied up to the incident." Some internal window dressing was in order.

The company has overseen the resignation of three senior managers in the rattled security unit, one stacked with 500 employees. On the chopping block was Pooja Ashok, chief of staff for the now sacked chief security officer Joe Sullivan; Prithvi Rai, senior security engineer, and Jeff Jones, responsible for physical security.

The security team has not covered itself in glory. Tasked with the onerous brief of keeping the company accounts secure, it has also been accused of engaging in pilfering programming codes and trade secrets from rivals. That particular case involves a $1.8bn litigation standoff between Uber and Alphabet's autonomous vehicle unit Waymo.

This ongoing battle has been illuminating on several levels. Uber's approach to regulation – its evasion, that is – has come out for some testing. Presiding Judge William Alsup was in a far from affable mood to Uber's general counsel in failing to disclose a 37-page letter suggesting the presence of a "shadow system" designed to avoid paper trails on supposedly sensitive information.

The question to preoccupy the legal fraternity now is whether the hack should have tangible consequences for Uber. In various states, customers and Uber drivers are looking at legal options over the data breach that may well be grounded in statutory form. The UK law firm Leigh Day has revealed that it had fielded inquiries from 10 disgruntled customers.

Law partner Sean Humber has certainly had his interest piqued by the possibility of a class action.

> "If private, confidential information has been mishandled, that could be a breach of the Data Protection Act, and people could have a claim under the act."

The line taken by Humber is eminently sensible: that Uber could well have facilitated a misuse of private information or, at the very least, a breach of confidence.

> "If people have suffered distress or loss as a result of that data breach, in principle they are entitled to compensation."

In Los Angeles, the Wilshire Law Firm was also keeping busy on this new frontier of litigation, filing a class action in the federal court claiming that the firm's drivers and passengers are at risk of fraud and identity theft.

This would be fitting. Uber is a company hell bent on global reach, and is happy to undercut local regulations, not to mention the taxi market, where possible. In various locales, the company is meeting forms of resistance.

In September, Transport for London refused the company's request for a new license, citing its app was not "fit and proper". TfL's reasons also included inadequate reporting procedures for serious criminal offences, the obtaining of medical certificates and the use of the Greyball software.

In other jurisdictions, the company has been banned on grounds spanning unfair competition to sidestepping local tax meters. But this is a conflict of monumental proportions waged in the courts and jurisdictions of the globe.

Uber, so far, has shown an appetite for donning its armour and going into battle. Domination does come with its fair share of bruising and flesh wounds. Importantly, as far as class actions are concerned, the company may well be able to shore up its defences in shifting the onus back to riders and drivers.

According to the 2nd US Circuit Court of Appeals ruling in August this year, the rider must agree to waive their entitlement to litigate in signing for the ride-sharing app. This also comes with an arbitration agreement clause activated on signing, though it does come with

an option to opt-out. That very attention to detail eludes most users of the system, the cost of near instance convenience.

Such deft trickery did not bother Judge Denny Chin, who wrote the judgment assented to by Judges Reena Raggi and Susan Carney.

> "While it may be the case that many users will not bother reading the additional terms, that is the choice the user makes. The user is still on inquiry notice."

Whether such cases protect the company from cases of gross negligence regarding the handling of user data is a point that still requires a firm answer. The firm's vast wings may well be, over time, clipped.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

---