White collar crime and metadata: beware of building a new honeypot

Published: February 27, 2015 6.31am AEDT

Author

1. John Selby

   Lecturer - Faculty of Business and Economics, Macquarie University

With the struggle by law enforcement agencies to keep pace with new technologies has come calls by the agencies for additional investigatory powers.

The call for communications service providers to retain two years of their customers' metadata is simply the latest round in this debate. While much of the current discussion has centred on consumer data and policing agencies, the proposal also covers the communications of businesses, and the Australian Securities and Investments Commission (ASIC) is one of the agencies seeking access.

Analysing two years' retained metadata about your communications would give any law enforcement agency enormous insight into your life and, potentially, leverage over you. Using the data they could easily identify completely legal but otherwise embarrassing confidential events in your life, such as whether you have, for example, had an affair, an abortion, called a suicide help-line, a brothel or alcoholics anonymous.

Having the power to analyse two years' retained metadata about a business' communications creates different risks: for example, knowing whether the senior executives of a listed company are talking often with a bankruptcy advisory firm or an investment bank's mergers/acquisitions team could create enormously valuable trading opportunities prior to the release of that information to investors and the general public.

The benefits of granting additional powers designed to increase the efficiency of law enforcement agencies need to be balanced against a range of risks, including the need to protect civil liberties and the possibility of unintended consequences.

What ASIC wants

The government's current plan for data retention law includes provisions which would limit which law enforcement agencies could gain warrantless access to the retained metadata. In its submission to the Parliamentary Joint Committee for Intelligence and Security Inquiry into Data Retention, ASIC argued the proposed Bill would reduce its existing powers to access telecommunications data and stored communications for the purposes of investigating white

collar criminal activities, such as insider trading, market manipulation and financial services fraud.

Over the last five years, ASIC has secured convictions against 129 people for serious offences under the Corporations Act (including sentences of more than 13 years' incarceration in some instances) and 2404 people for less serious offences, though it did not specify how many of these convictions depended upon evidence gained from metadata.

ASIC currently has access to telecommunications data under sections 178-179 of the Telecommunications Interception Act. It claims it has used that information in over 80% of its insider trading investigations, including in the Lucas Kamay (NAB) and Christopher Hill (ABS) case.

ASIC uses a variety of techniques to investigate white collar crimes, including data analytics of trading patterns. It also receives reports of suspicious trading activities from industry participants and the general public.

Metadata is particularly useful for ASIC when seeking to identify potential suspects (and their accomplices) and their methods/patterns of communication, so that further surveillance of ongoing behaviour can be undertaken. While metadata itself does not definitively prove the identity of who was talking on a particular phone, typing a text message or sitting behind a keyboard, it can suggest who was most likely to have been doing those things (i.e. in many cases, the registered owner of the account). The actual identities of the participants can then be confirmed through follow-up surveillance.

Metadata can provide information on the methods that two or more people are using to communicate (whether by landline, mobile phone, SMS, Skype, etc). It can also provide a rich history of both patterns of communication (which devices are in contact with which other devices, when and how often) and interruptions to such patterns of communication, such as ceasing to communicate by mobile phone or changing phone SIMs, which could indicate the suspects believe they are under surveillance.

In some trials, evidence of the timing of communications can be critically important. For example, when NAB trader Lukas Kamay received confidential information from Christopher Hill about yet-to-be-released Australian Bureau of Statistics' data, Kamay was able to profit by placing leveraged foreign exchange trades on the value of the Australian dollar. ASIC only became aware of this activity after it was tipped off by Kamay's forex brokerage firm, Pepperstone Financial, and while access to metadata played a small part in the investigation, it was traditional surveillance which resulted in the convictions of Kamay and Hill.

Access to retained metadata would grant ASIC the ability to search the history of patterns of conduct between suspects, such as whether they were repeatedly communicating and trading just prior to the announcement of market-sensitive information, even in situations where ASIC only became aware of the possibility of illegal activities well after they had actually occurred. It may also assist them to identify additional co-conspirators.

A new honeypot?

To be able to undertake such analysis, ASIC would need metadata to be retained from businesses as well as from individuals. Under the Bill, such metadata would be stored by communications providers, such as mobile phone companies and ISPs. This poses a risk for some businesses as their communications metadata contains highly valuable confidential information.

In its drive to increase the effectiveness of its fight against white collar crimes, it is possible ASIC and the government may unintentionally increase the risk of such crimes occurring while also making them harder to detect.

Communications service providers forced by the proposed legislation to store metadata are likely to provide security sufficient to protect against unauthorised access based upon the risk profile of their average customer, rather than for their most-at-risk customers. This raises the possibility of third parties seeking to gain unauthorised access to businesses' financially sensitive information through their retained metadata, whether third party hackers using zero-day exploits, or trusted public servants (like Hill) looking to supplement their government pay cheques.

Insider trading and market manipulation may become harder to detect because third party hackers will no longer need to directly attack listed companies and their advisers, but instead could indirectly gain information by attacking metadata repositories. If a communications service provider pooled all of its customers' metadata into a single database, then this may represent the equivalent of an inadequately secured goldmine for white collar criminals.

We should not rush to implement a system of metadata retention before all of the costs and benefits of such a proposal are fully considered.

Disclosure statement

John Selby is also affiliated with the UNSW Cyberspace Law and Policy Community, other members of which made separate submissions to the PJCIS Inquiry into Data Retention. In 2001, he was seconded as an in-house counsel for Telstra's Retail eCommerce legal team. He previously worked as an Internet lawyer for Mallesons Stephen Jaques (now King & Wood Mallesons).

Partners: Macquarie University provides funding as a member of The Conversation AU.

URL: <https://theconversation.com/white-collar-crime-and-metadata-beware-of-building-a-new-honeypot-37891>