Metadata capabilities spark global privacy concerns

Friday, June 21 2013

Metadata, the information gathered by the US National Security Agency (NSA) from telephony and internet companies, has been the focus of ex-NSA contractor Edward Snowden's disclosures. Senator Dianne Feinstein, chairman of the US Senate Select Committee on Intelligence, has sought to reassure the public that their names and the content of their conversations were not handed over by Verizon (and presumably other US telecoms) -- only the metadata. However, metadata is more invasive and useful to surveillance agencies than this suggests, potentially revealing more about an individual's private life than direct eavesdropping.

A man checks his mobile phone (Reuters/Anindito Mukherjee)

What next

US and international civil liberties groups are calling for an end to government agencies' collection and aggregation of metadata; however, unless there is sustained public pressure, the eventual legislation risks being watered down -- and the prospects for reform in the United States are particularly poor. Despite the initial backlash and efforts by internet-based companies to restore consumer confidence in their privacy policies, in the long term privacy concerns will be superseded by the convenience of these services for consumers.

Analysis

Metadata is not the content of a phone or email conversation. Instead, it comprises all of the additional information created in the background as a user employs technology; it is detail about the activity, rather than the content.

Metadata of a phone call includes:

- the phone number of the caller and receiver;
- the location;
- the time the call was placed;
- the duration of the call; and
- the unique serial number of both phones.

The metadata of an email consists of:

- the name of both the sender and recipient;
- email addresses;
- the date and time of sending; and
- the sender's timezone.

Impact

- The surveillance revelations undermine US policies promoting online freedom.
- Knowledge of the surveillance will fuel expansion of sophisticated, encrypted leaking systems by news organisations to protect sources.
- This will also encourage the development and use of anonymisation tools, such as disposable unregistered phones.
- It could also steer governments to create their own state-funded data storage infrastructure to safeguard their citizens' data.

Metadata is, to a large extent, more valuable than the content of a call or email. Tracking a chain of communication, combined with location data, when aggregated can reveal details of an individual's life. Cross-referencing with other data sources can complete the picture. It is no surprise that metadata is valuable, given the number of internet and technology companies that have built their businesses around collecting and exploiting it (see INTERNATIONAL: Internet firms disrupt wider markets - June 20, 2013).

Patterns in metadata

Analysed metadata can reveal behavioural patterns, exposing personal or hidden information

Security services may analyse metadata with the intent of revealing a terrorist cell. However, chains of phone calls (A calls B, who then calls C and D) coupled with location data can also uncover legal, but secretive meetings, such as political or corporate negotiations, or journalists meeting sources. Last November, David Petraeus, then CIA Director, resigned after the revelation of his extramarital affair with Paula Broadwell. The affair was discovered through the use of metadata, but was not the FBI's intended target; rather, there were concerns of a security breach. This provided probable cause to monitor Broadwell's email accounts, subsequently revealing the affair.

Automated pattern analysis on metadata could increase incidents like the Broadwell flap. Notwithstanding that automated analysis enables widespread monitoring without the need to expand the workforce, it also removes the need for human oversight, increasing the risk that innocent behaviour may be misinterpreted. Furthermore, advancements in data storage capacity permit governments to keep data indefinitely. While this could be useful for cross-referencing over a longer period of time, it could nonetheless create an extensive database of citizens' private lives.

Public or private data?

No warrant was necessary to collect the initial email metadata that led to Broadwell's identification because metadata is regarded as public, not private, information. Responding to the NSA metadata collection, Feinstein stated that US courts consider that "there is no reasonable expectation of privacy in this type of metadata information".

Whether metadata is public or private is ambiguous

However, whether metadata is public or private is not quite as clear as this suggests. Certainly, citizens do not expect full privacy for their data -- they are willing to trade it with companies for convenient services -- but they are less comfortable with giving the state access to it. The state can aggregate data to a far greater extent and use it for potentially more invasive purposes, such as criminal proceedings.

There is an assumption that the 'Millennial' generation (those currently aged 18-29), as digital natives, is less concerned about privacy than older generations. This stems from their apparent willingness to share information about themselves -- thoughts, photos, their immediate location -- online. This ignores the importance of perceived control in the user/provider arrangement. People allow companies to use their data in exchange for services; they are knowing participants in this arrangement.

By contrast, governments claiming access to the same data is unilateral: there is no reward through use of services, and no privacy/sharing settings to give users a sense of control. Nor is there a tangible product that derives from this access (such as targeted adverts). Instead, governments' data mining for security is abstract, obscuring the potential implications this may have for users.

International concern

The scope of the NSA's metadata collection has prompted international unease. The European Council highlighted as a particular concern the aggregation of EU citizens' data, who do not benefit from the protections afforded to US citizens. This presents a potential challenge for ICT businesses, since European data protection laws can require companies to show how collected data is used, and to which organisations it may be passed (see EUROPEAN UNION: Privacy spat leads to new data regime - March 13, 2013).

Corporate reputational damage

Amazon secured a contract with the CIA for a cloud computing system worth 600 million dollars

Suggestions that US internet companies have close relationships with US government agencies is also damaging to their businesses (see INTERNATIONAL: Foreign policy joins corporate toolkit - February 15, 2011). They weaken international customers' confidence in the security and privacy of US-based internet and technology companies. The companies involved now face a difficult balancing act, allaying consumer concerns over privacy by publicly downplaying their cooperation with the NSA without jeopardising their relationships -- and for some their lucrative contracts -- with these government agencies.

Almost all have since released 'transparency reports' in an attempt to counter speculation that they provide unfettered access. Thus far, these reports have proven limited and problematic when scrutinised. The national security requests are obscured by being included in the overall figure for law enforcement requests, and this figure itself is significantly lower than the leaked documents suggest. Google even brought a legal challenge to the order that prevents it from revealing the precise number of requests.

Consumer and business data storage is increasingly moving away from local, private computers to the 'cloud'-- services or software provided and accessed remotely over the internet. While the convenience offered by cloud services will continue to appeal to individual consumers and businesses, they will need stronger reassurances concerning the security and privacy of the data held for them by third parties.