When does Google hand over your data to governments?

September 19 2014, by Nicolas Suzor And Alex Button-Sloan

What data from telcos and tech companies does the government want handed over? Credit: Flickr/Nic McPhee , CC BY-SA

Governments around the world want to know a lot about who we are and what we're doing online and they want communications companies to help them find it. We don't know a lot about when companies hand over this data, but we do know that it's becoming increasingly common.

Google has released its latest Transparency Report which shows a rapid increase in the amount of requests it receives for access to private data.

Google isn't alone in publicly releasing this kind of data. A few other major players such as Yahoo, Vodafone, Apple, Facebook, Microsoft and Dropbox have also published statistics about the requests they receive to provide personal details of their users.

Some providers, such as Twitter, have built a reputation for resisting government requests for information - but even Twitter ends up complying most of the time.

It's hard to resist: recently released documents reveal that Yahoo was threatened with a massive US$250,000 per day in fines if it didn't hand over data to the National Security Agency (NSA), enough to bankrupt it within a few months.

Australian police are hungry for more data

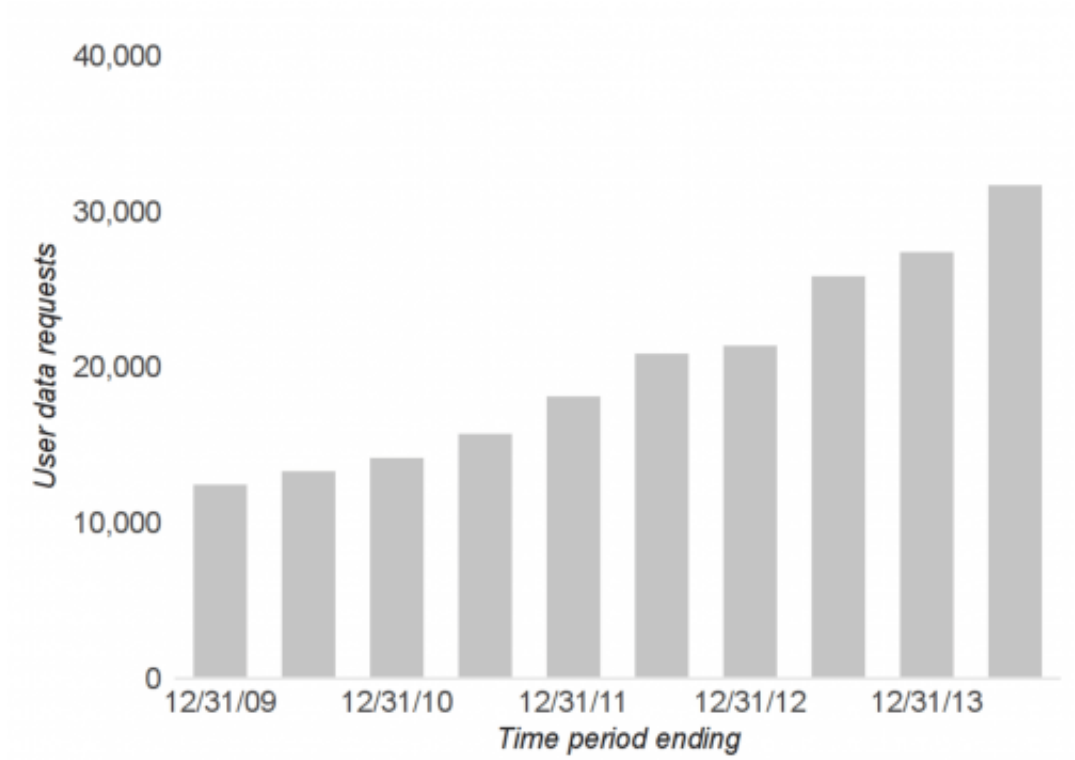
Google's report shows that requests for information about Australian users have nearly tripled since 2010.

These figures are tipped to keep rising, as the Australian Government pushes to impose "data retention" obligations on internet service providers and telecommunications companies. The recent counter-terrorism operations in Queensland and New South Wales are expected to strengthen the political argument for the government's plan.

Under these data retention proposals, companies will be required to store customers' internet and phone data for up to two years. During this time, law-enforcement and intelligence agencies can request access to an unprecedented amount of data about our online activities.

The government says these requirements are necessary to fight local terrorists. But they have been heavily criticised by industry and privacy groups.

The sheer amount of data to be indiscriminately stored under the proposed scheme raises serious questions about the rights of ordinary Australians whose every online action will be open to scrutiny.



Requests from government agencies worldwide for user data from Google. Credit: Google

Storing all of this data will also cost a lot, making internet access more expensive for consumers. Most worryingly, there is little to stop these huge stores of data being used inappropriately by officials, or ending up

in the hands of hackers or foreign surveillance agencies.

No oversight or protection for privacy

A large part of the problem is that Australian law provides few restrictions on how government agencies request private data from telcos and internet service providers (ISPs). The Telecommunications Act includes broad provisions that allow requests for data to be made by the Australian Security Intelligence Organisation (ASIO) and law-enforcement agencies.

Another controversial part of the Act, Section 313, requires telcos to give State, Territory, and Commonwealth officials "such help as is reasonably necessary" to enforce criminal laws and civil penalties.

These powers are not limited to require government agencies to get a warrant or court order to access private information. Requests for access are not just limited to domestic terrorism, but will inevitably be used in routine law enforcement investigations.

Such easy access to data about our online activities represents a massive shift towards routine surveillance. Without judicial oversight, we are placing an extraordinary amount of trust in government agencies not to abuse their powers.

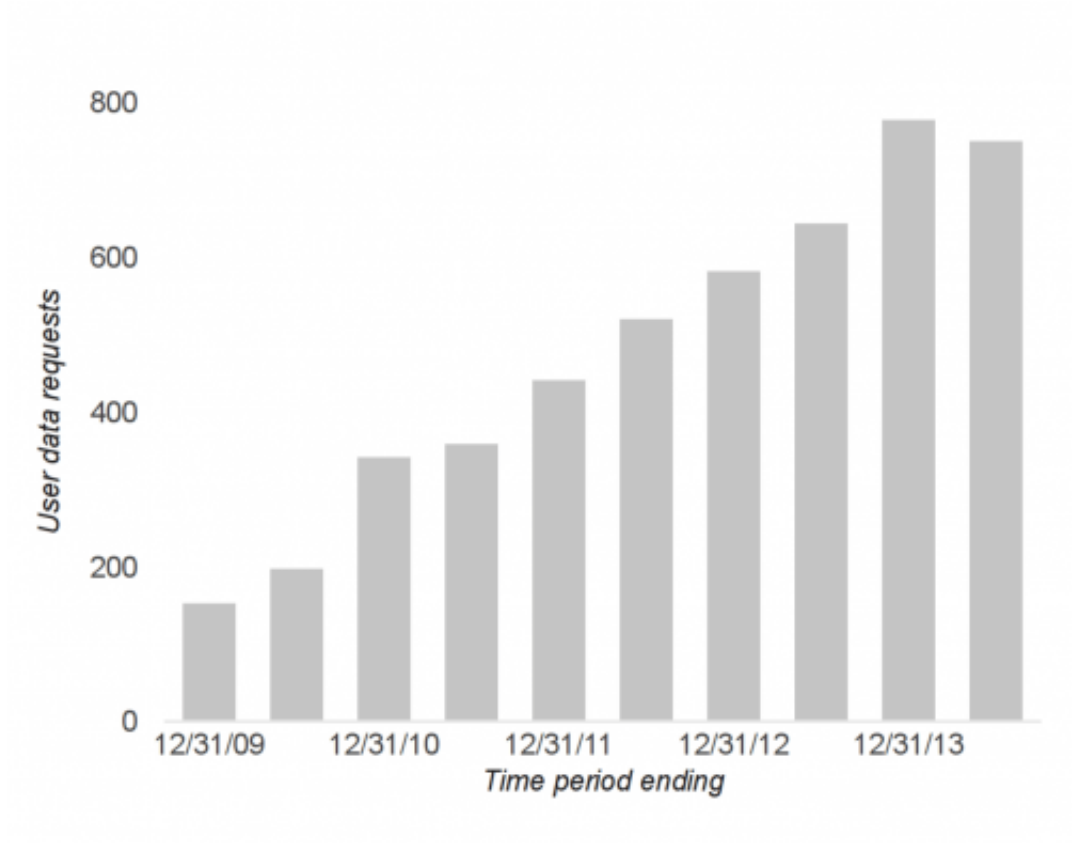
Private censorship requests

These transparency reports also highlight another difficult problem. Online service providers are also increasingly being asked to remove or disable links to content that others have posted.

While these requests vary according to the laws of various countries,

they usually concern material that is defamatory, offensive, breaches privacy rights or infringes copyright.

The difficulty with these requests is that intermediaries such as Google are poorly placed to evaluate whether a particular piece of content breaches the law. That's a question that we have always previously left to courts to decide.



Requests for user data from Australian authorities. Credit: Google

But the issue is not that simple. Many advocacy groups have complained that by the time victims apply to a court to have material removed, it's just too late - the harm has been done. From issues such as hate speech,

to leaked nude photos, many think that organisations such as Google should do more to police the internet.

Greater transparency needed

These are complicated issues. We clearly want law enforcement agencies to be able to investigate crimes, but we also want our privacy to be protected. We want people whose privacy has been breached, or people who suffer from stalking or bullying, to be able to get links to offensive material removed from the web.

But we also want to protect legitimate freedom of speech, and we don't necessarily think that private organisations are best placed to make the distinction.

In order to work through these conflicts, the first thing we need is more information. Currently, only a handful of service providers around the world provide reports on the requests that they receive from law enforcement and private citizens, and government agencies rarely provide good information themselves.

There is much we still don't know about how our data is being accessed or how complaints are dealt with. We often only have high level statistics and little detail about the process under which decisions are made to comply with or refuse requests.

Ultimately, there are no easy answers to the role that service providers should play in enforcing the law. But there is one easy answer: we deserve to know what is happening to our data and how our laws are being enforced. Transparency is a key requirement for a democratic society.

Commons-Attribution/No derivatives).

Source: The Conversation