SECURITY MEASURE:
Law enforcement agencies want access to internet data

WHO'S WATCHING

BALANCING PRIVACY AND SECURITY CAN BE A TIGHTROPE WALK IN THE ONLINE WORLD.

Story: **Jeremy Kennett**

It's late 2009 in Dallas, Texas, and Hosam Smadi is about to blow up a 60 storey skyscraper. He takes out his phone, ready to dial a number linked to a massive truck bomb. Maybe he says a prayer. Maybe he's scared, angry, joyful – no-one knows. What is clear is what happens when he makes the call: nothing.

Nothing, that is, until FBI agents swoop moments later, arresting him for attempting to carry out a major terrorist attack. It turns out the Al-Qaeda 'sleeper cell' Mr Smadi had thought was helping him plan and prepare for the attack was actually a group of undercover FBI agents who had been monitoring him since he made extreme pro-violence posts on a radical Islamic website.

Mr Smadi received a 24-year sentence in 2010 for his crimes. Case closed, crisis averted.

But what might have happened if the FBI had never found out about Mr Smadi's plans? Or if they hadn't been able to find out his identity based on his online threats?

> "Telecommunications data forms the foundation for almost every serious investigation and is a significant element of the evidentiary process."

Internet monitoring by law enforcement agencies was crucial in the Dallas operation, from identifying the initial threat to building trust with the target and ultimately preventing a tragedy. Without access to data identifying Mr Smadi he might never have been linked to his violent statements and the next terrorist cell he came across may have been genuine extremists.

It's this sort of risk which has led Australia's law enforcement and intelligence agencies to support an unprecedented increase in access to the internet and phone data of Australians.

Photos: **iStock, aapone & newspix**

DATA RETENTION:
Information collected could assist with investigations

Chief among a number of changes outlined in a discussion paper on reforms to national security legislation is a proposal to require telecommunications companies to retain data on the internet and phone usage of all Australians for a period of two years. This data would then be made available to relevant law enforcement agencies to assist their investigations, provided they have satisfied authorisation procedures for access.

In a joint submission to the parliamentary inquiry reviewing proposed reforms to national security legislation, the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO) and the Australian Crime Commission (ACC) say this sort of data is essential to the majority of their investigations.

"Loss of access to such data, for technical or legal reasons, would result in a loss of a fundamental investigative capability and the ability of security and law enforcement agencies to function effectively," the submission states. "Should data retention not proceed, we anticipate that almost every security intelligence and serious crime investigation undertaken by ASIO, the AFP and the ACC (and by state police) will be affected.

"Telecommunications data forms the foundation for almost every serious investigation and is a significant element of the evidentiary process."

However the proposal has been labelled as extreme by a range of organisations, community groups and individuals, with many concerned the AFP and other agencies are seeking to ensure our security by sacrificing our freedom.

Victorian Privacy Commissioner Dr Anthony Bendall says the proposed data retention scheme is characteristic of a police state.

"It is premised on the assumption that all citizens should be monitored," Dr Bendall says. "Not only does this completely remove the presumption of innocence which all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life."

Dr Bendall acknowledges privacy is not an absolute right, and needs to be balanced with the public interest in protecting the safety and security of Australians. But he quotes the first Victorian Privacy Commissioner Paul Chadwick to warn "fear can make us welcome what should be only reluctantly and warily tolerated".

"A democratic nation is not secured by compromising, any more than strictly necessary, the freedoms that allow a democracy to function," he says. "Preserving freedoms under law is part of what it means to guard the national security of a democracy.

"To diminish freedoms unnecessarily or disproportionately makes the nation insecure."

His words are echoed by Stephen Blanks, secretary of the NSW Council for Civil Liberties. Mr Blanks says the proposal would fundamentally change the relationship between the state and the individual in Australia.

"This proposal involves turning telecommunications companies into data collection agencies for the government," he says. "It involves collecting data from individuals which

"To diminish freedoms unnecessarily or disproportionately makes the nation insecure."

CAUGHT IN THE WEB:
Critics worried about creating a security state

is not required for any legitimate business purpose, just so it can be handed over to government.

"It's another big step to turn a democracy into a security state."

Part of the concern has been caused by the lack of detail given about how the data retention scheme would work and what it would cover.

The proposal takes up just three sentences in the 61 page national security legislation discussion paper, among a group of proposals on which the government is expressly seeking the views of the committee. It calls for "tailored data retention periods for up to two years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts".

A number of critics of the proposal have interpreted this to mean any type of information could be retained, including the content of communications and lists of visited websites and web searches.

The AFP, ASIO and ACC have moved to allay these concerns by making it clear in a supplementary submission to the inquiry they are not seeking to record the web content or browsing history of all Australians.

Rather they are interested in communications data or 'metadata', which includes information like telephone numbers, email and internet protocol (IP) addresses and other similar information that would allow them to identify the people involved in a communication.

The agencies say this sort of data is vital when investigating suspicious activity, but is currently inconsistently recorded and retained by telecommunications companies, making mandatory data retention necessary.

But Civil Liberties Australia director Tim Vines doesn't accept the agencies' claims they won't be able to see the content of communications and web histories.

"The limitation is supposedly that what we're looking for here is communication data – who you're contacting but not what you're saying to them," Mr Vines says. "Now from a technical perspective that doesn't really make any sense.

"Because when you're talking about an IP address of your computer and the person you're trying to contact, that's the website. An IP number is just the fundamental information that sits behind a URL. So really IP addresses are still your web history.

"People who have a background in the industry, who understand the types of information they're talking about have had a look at these proposals, they've baulked at the suggestions and they've said actually you really need to clarify what you mean here."

One industry expert with concerns about the proposal is Internet Society of Australia president Narelle Clark, who has more than 20 years' experience as a telecommunications engineer. Ms Clark says assurances by agencies that they are only seeking metadata are meaningless given the lack of a clear definition of what that means.

"So far the only information we've received from the Australian Federal Police, that describes what metadata is, is so lightweight as to be completely ineffective," Ms Clark says.

"Indeed internationally there are no technical standards for what metadata is.

"So it looks to me like a fishing expedition. If there is no clear definition that we can work with at this stage then there is no way we can rule anything in or anything out.

"Indeed as I've said the proposal that we've received so far from the Australian Federal Police is so vague that it could encompass anything and everything, or nothing."

Ms Clark also has concerns about how telecommunications companies would be able to secure the retained data, which may be very attractive to both criminal and commercial enterprises. She says telecommunications companies will be unable to absolutely guarantee the security of personal data, no matter what the requirements.

"I would say it is impossible to secure any piece of data that is kept on a computer that is turned on," she says.

While measures can be taken to increase the security of the data, the attractiveness of the information to criminals could lead to determined hacking efforts.

"These sorts of systems will become very, very attractive both commercially and in other realms. So the risk of this system becoming available to people who want to do harm is also proportionally raised."

Data security has also been identified as an issue by the law enforcement and intelligence agencies, which say more stringent requirements need to be placed on telecommunications companies.

"The protection of this data remains paramount and is one of the main drivers behind the proposed Telecommunications Sector Security Reform which aims to increase the level of security in telecommunications networks," the agencies' submission states.

However the telecommunications companies themselves have warned extra security and retention requirements will come at a high price.

The Australian Mobile Telecommunications Association and Communications Alliance estimate that the cost to industry of setting up a basic data retention scheme would be at least $100m, rising to as much as $700m if source and destination IP addresses are required to be retained as is proposed.

> "At least four planned terrorist attacks designed to achieve mass casualties on Australian soil have been thwarted by agencies since 11 September 2001."

As well as seeking assurances that these costs will be borne by government and not by industry, the alliance shares the concerns of the Privacy Commissioner and others about the privacy and security costs of the proposal.

"Industry believes it is generally better for consumers that service providers retain the least amount of telecommunications information necessary to provision, maintain and bill for services," the alliance says.

It also believes the data retention scheme could lead to even greater privacy invasions when combined with other government initiatives.

"Consider, for example, the inclusion of a requirement to capture and retain the location of mobile customers, as has been proposed as part of the Department of Broadband, Communications and the Digital Economy's Integrated Public Number Database review.

"With the addition of a data retention obligation, this could be expanded into an ongoing surveillance regime capable of tracking the movements of all mobile customers."

SAFETY FIRST:
Balancing privacy and security

Tightening laws covering the security of telecommunications networks is just one of a raft of reforms to national security legislation suggested in the discussion paper – changes that go far beyond just the proposal on data retention.

Another suite of changes centres on the issuing of warrants to intercept communications and conduct searches of the homes and property of suspects. The discussion paper calls for the standardisation of tests and thresholds for telecommunication intercept warrants, as well as the streamlining and modernisation of ASIO's warrant provisions.

In practice this would mean agencies would be able to get multiple telecommunications interception powers under a single warrant, rather than needing to apply for a separate warrant for each power. ASIO would be able to use this single warrant process for powers beyond interception.

The discussion paper claims the changes are necessary to ensure warrant processes are flexible enough to respond to the changing telecommunications environment.

"The Telecommunications (Interception and Access) Act is based on an assumption that there is a unique, non-ambiguous identifier, such as a phone number, linking the target of an interception warrant to the service (or device) to be intercepted and in turn to the carrier required to give effect to the warrant," the paper states.

"However, typically there are no longer clear, one-to-one relationships between the target of an interception warrant, telecommunications services used by the person, and telecommunications service providers because users of telecommunications services may have multiple 'identities', each of which may only be meaningful to a particular service provider.

"Persons seeking to avoid surveillance commonly exploit this situation."

But the Gilbert and Tobin Public Law Centre at the University of New South Wales warns standardising warrant

The cost to industry of setting up a basic data retention scheme would be at least $100m, rising to as much as $700m

requirements may weaken accountability if the thresholds for more intrusive powers, such as installing listening and tracking devices, are lowered rather than those for less intrusive powers being raised.

The centre is also concerned about moves to extend the validity of ASIO search warrants from 90 days to up to six months, saying it is an example of how a focus on streamlining and simplification can override concerns about the civil liberties of the individual.

"The vast majority of ASIO warrants may operate for a maximum of six months," Gilbert and Tobin says in its submission.

"Search warrants, in contrast, only operate for a maximum of 90 days. There is a rational reason for this distinction. Searches, whether of premises or of person, are far more intrusive than the other ASIO warrant powers. As a consequence, there should be greater control over search warrants by the issuing body.

"This is not a disproportionate administrative burden given the significant inroads that searches make into the individual's right to privacy."

There's no doubt the privacy of Hosam Smadi, the would-be Texas bomber, was infringed upon by the agencies who investigated him after he made violent comments online. In that case most people would probably agree that preventing a potentially catastrophic terrorist attack was worth the intrusion.

But whether that holds true for the data retention scheme and other proposals put forward in the discussion paper is still far from settled.

While the debate continues, the proponents of change say action is needed now to ensure new technology can help agencies stop crimes and acts of terrorism, rather than help shield their perpetrators from justice.

"In the absence of action, significant intelligence and evidence collection capabilities will be lost providing criminal elements with a technological upper hand," the AFP, ASIO and ACC state.

"Australian intelligence agencies have made a significant contribution to our safety by constant and careful assessment of possible threats. At least four planned terrorist attacks designed to achieve mass casualties on Australian soil have been thwarted by agencies since 11 September 2001.

"To continue this crucial role, it is imperative that Australia's intelligence agencies remain robust and can effectively deal with the challenges presented by today's and tomorrow's international security environment." •

For more information on the inquiry by federal parliament's Intelligence and Security Committee into potential reforms of national security legislation visit **www.aph.gov.au/pjcis** or email **pjcis@aph.gov.au** or phone **(02) 6277 2360**.