Protecting Privacy: **Is it too late?** OVERVIEW

Huntsman®
Defence-Grade Security Platform

'IS THE AGE OF PRIVACY OVER?'

That is what Facebook founder Mark Zuckerberg told an audience back in 2010. In 2013 we saw the largest data breaches ever (Target, JP Morgan and Home Depot customer data compromised). Earlier this year eBay confirmed that its customer database, including passwords, had also been hacked.

It is not just criminals who want to know more about us: Some governments and companies like Google, Apple and Facebook do too. As a result, our privacy is under siege.

BIG DATA TO BIG BROTHER?

A Sydney Morning Herald article reports that global mall operator Westfield in Australia is monitoring the movements of smartphones belonging to shoppers; yet apparently this does not breach privacy laws. Meanwhile, Google has received a patent for a 'head-mounted device' (Google Glass) that tracks what wearers are looking at and offer personalised 'pay-per-gaze' advertising.

Governments are also monitoring millions of citizens, as shown by Edward Snowden's revelations about the surveillance programs conducted by US and UK intelligence agencies.

THE PERSONAL DATA ECONOMY

'A child born in 2012 will leave a data footprint detailed enough to assemble a day-by-day, even a minute-by-minute, account of his or her entire life, online and offline, from birth until death...,' Mark Sullivan writes in PCWorld.

Most large Business to Consumer (B2C) companies now have predictive analysis sections that comb through the data they hold or purchase about us. Disturbingly, just like a honey pot, the more data they collect, the more appeal they have for hackers.

'LEARNING TO HATE BIG TECH'

Facebook has admitted that it scans conversations for evidence of criminal behaviour, while Twitter, Apple and other mobile app makers have been accused of uploading user address books without their permission.

It is well known that Google has faced a number of investigations regarding its 'Street View' program, when it was revealed that camera cars were gathering private data. Google was also caught out circumventing the privacy settings in Apple's Safari web browser, an action that attracted a multi-million dollar fine from the US Federal Trade Commission.

In a piece headed 'Learning to Hate Big Tech,' Time Magazine asked the obvious question: 'Is big tech replacing the big banks and Wall Street as the corporate villains du jour?

It is not just criminals who want to know more about us: Some governments and companies like Google, Apple and Facebook do too. As a result, our privacy is under siege.

TOUGHER RULES, LANDSCAPE AND TECHNOLOGY

For organisations that operate in multiple geographies, the uneven legal terrain of privacy protection presents additional challenges. While the regulations governing privacy are being reinforced across the globe, IT environments are becoming harder to control due to the growing number of smart mobile devices, and the increasing use of cloud services for accessing and storing data. To give your enterprise the best chance of managing this environment, you will need greater vigilance, tighter controls and smarter technologies.

Whether you use DLP, MDM or classification and labelling of critical data as part of your privacy protection strategy, it is vital to maximize their functionality with advanced capabilities that are up to the challenge. In the context of privacy, these capabilities include:

- scalable log collection, automated log analysis, log management and reporting for complete visibility and audit;
- ability to collect, aggregate and correlate data from mobile devices and other network data to ensure real-time whole-enterprise monitoring; and
- behavioural analysis like Behaviour Anomaly Detection (BAD) which baselines normal activity and alerts in real-time on the unusual.

THE BOTTOM LINE

A common factor amongst most privacy regulatory regimes is a need to be able to detect breaches when they occur. Where breaches are picked up by third parties, customers or regulators directly it is very hard to defend a duty of care and even harder to regain the initiative in the resulting response.

Huntsman® allows a comprehensive and proactive monitoring regime to be established so that organisations are able to detect issues more quickly, can avert disruptive clean-ups and economic loss. In doing so Huntsman® users can reduce compliance costs, limit fines and avoid the reputational damage that a privacy breach can increasingly entails.

REFERENCES

1 Tracked from the moment you wake, SMH, August 24, 2013

2 How Pay-Per-Gaze Advertising Could Work With Google Glass, New York Times, August 20, 201

3 Data Snatchers! The Booming Market for Your Online Identity, PCWorld Security, June 27 2012

4 The Great Privacy Debate, CNET NEWS, July 17, 2012

5 Judge OKs $22.5m fine against Google for Safari tracking, CNET, November 19, 2012

6 Learning to Hate Big Tech, Time Magazine, May 14, 2012

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman