Computer Evidence 101 for Defence Lawyers

Ajoy Ghosh

Agenda

1. Introduction
2. Choosing an expert
3. Aspects of computer forensic evidence
   1. Reliable
   2. Relevant
   3. Sufficient
4. Data recovery
5. Mobile p

Every click you take, they'll be watching you

The law has a new high-tech stool pigeon reporting criminal activities, writes **Amber Hunt**.

Got an iPhone in your bag? Chances are you may be storing even more personal information than you realise, and some of it could be used against you if you're ever charged with a crime.

A burgeoning field of forensic study deals with iPhones specifically because of their popularity, the demographics of those who own them and what the phone's technology records during its use.

Two years ago, as iPhone sales boomed, a former hacker, Jonathan Zdziarski, decided law-enforcement agencies might need help retrieving data from the devices.

50 million iPhones, according to company figures. Clearing out user histories isn't enough to clean the device of that data, said John Minor, a communications expert and

mapping functions, as well as various global positioning system applications.

The free application Urbansgoon is primarily designed to help users locate

Thieves ensure raising goes off with bang

THE IMPOSTORS

THE REAL NICOLE McCABE

JOSHUA BRUCE'S MOTHER

"I am fearful, but hopefully everyone will see that it is fraud."

THE VICTIM

Facebook failed to tell police about paedophile porn ring

Dylan Welch

FACEBOOK management failed repeatedly to reveal the activity of an international child pornography syndicate operating on their site and ignored continuing admissions by one of the ring's Australian members.

The failure by the social networking site was uncovered during a federal police-led international investigation of the syndicate, which had been using fake online identities.

"We are aware that Facebook knew of the existence of these pages and even went so far as to remove the profiles," said the director of the AFP High Tech Crime Centre, Neil Gaughan.

But despite closing down the pages after finding illegal material, Facebook did not contact police, Mr Gaughan said.

"Facebook deactivated the online accounts of the initial suspects but there were indications that within hours, the groups were re-forming again."

The taskforce codenamed Project Ocean, was set up by the AFP in March. By June it included the FBI in the US, the Child Exploitation Online Protection Centre in Britain, the Mounted Po Germany, S Switzerland.

While off may have be involved in men have b include two aged 33 and

old from Port Kembla. The British-based man police say is the ringleader was due to face an English court overnight.

All 11 are accused of creating

company failed to pass the information to police.

Federal police also contacted a Facebook official in Australia to convey their concerns, and

tacted for comment yesterday. However, a Sydney public relations company that works for the company sent the Herald quotes made by the company's chief

TRACKING YOUR EVERY MOVE

- Every time an iPhone user closes the built-in mapping application, the phone snaps a screenshot and stores it.
- iPhone photos are embedded with tags and identifying information, so photos posted online might include GPS co-ordinates of where the picture was taken and the serial number of the phone that took it.
- Even more information is stored by the applications themselves, including the user's browser history, which could prove useful to police.

tories and text messages most useful in homicide cases. But Zdziarski, who has helped federal and state law-enforcement agencies

Apple doesn't store that cache very securely, Zdziarski contended, so someone with expertise could recover months of typ-

Why I'm up here

Lecturer:

- Law Schools at UNSW and UTS
- Santa Clara Law School
- Beijing Management College of Politics & Law

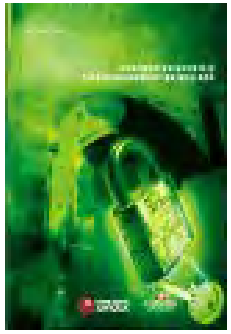
Expert witness in court:

- Civil: contract, evidence, reliability, authorship, times
- Complex criminal: terrorism, identity theft, fraud, stalking, data leakage
- Content: child pornography, terrorism, spam, harassment, vilification
- Serious criminal: homicide, rape, corruption

Litigation coach:

- Lawyers, judges, prosecutors
- International jurisdictions including alternative legal systems eg. ICC, China
- Preparedness specialist

HB171: Guidelines for the Management of IT Evidence (above)
HB231: Guidelines for Information Security Risk Management (below)



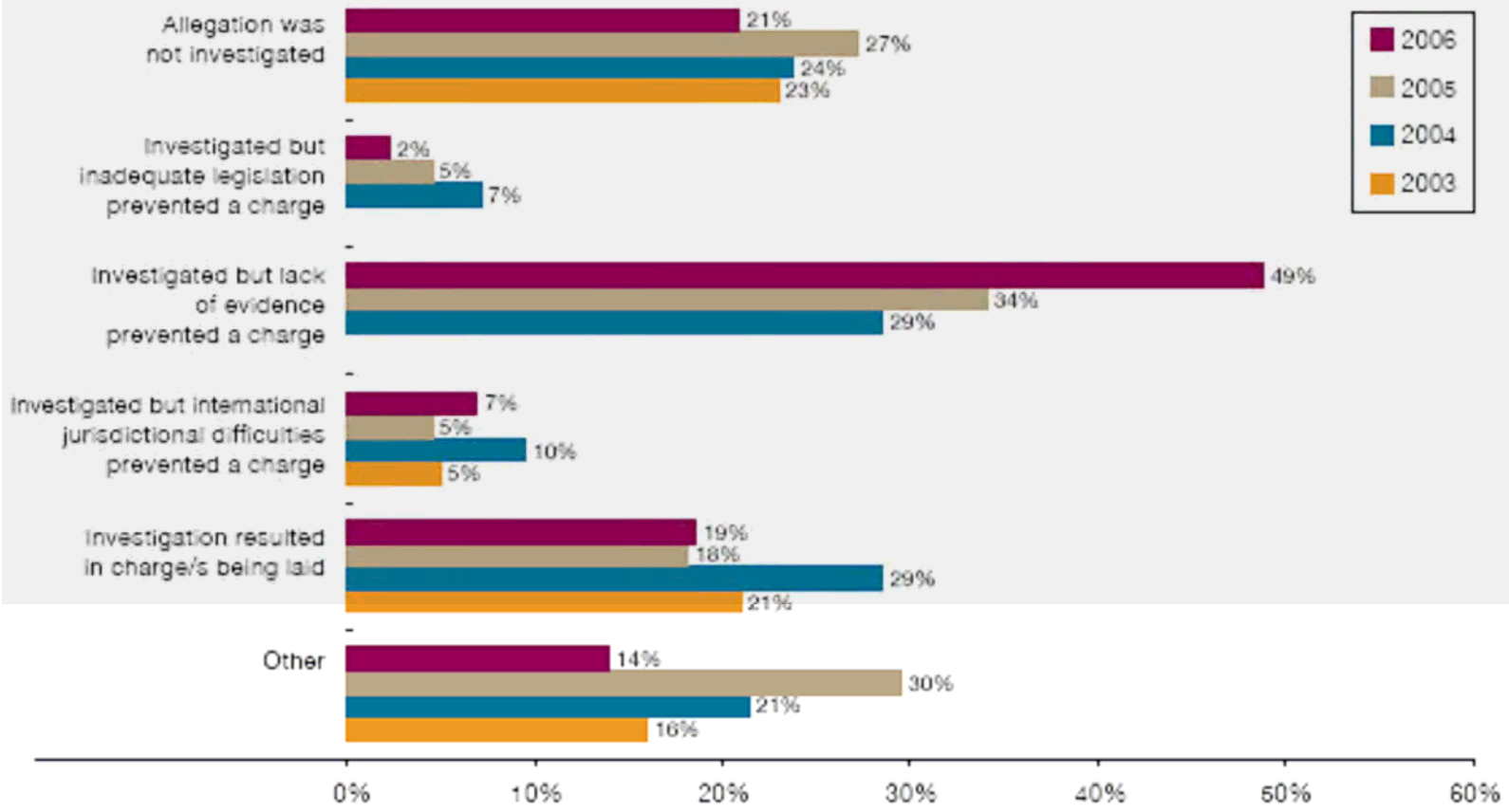
15+ years experience in information security, investigations and policy:

- Police, Corporate & Consultant
- Chief Information Security Office at Logica
- Senior IT Security Professional for 2009

Best practice:

- Author of HB171 – Guidelines for the Management of IT Evidence
- Co-author HB 231 – Information Security Risk Assessment Guidelines
- Currently working on ISO N9735 – Guidelines for identification, collection and/or acquisition and preservation of digital evidence
- CISSP and iRAP accreditations

Where electronic attacks or other forms of computer crime were reported to an Australian law enforcement agency, what was the outcome?



Source: 2006 Australian Computer Crime and Security Survey
2006: 43 respondents/11%, 2005: 44 respondents/24%,
2004: 42 respondents/18%, 2003: 61 respondents/28%.

Note: In 2003, "lack of evidence prevented a charge" and "inadequate legislation prevented a charge" were not options for this question.