DIGITAL EVIDENCE: DIGITAL REVOLUTION IN CRIMINAL CASES

NATHAN WHITEMAN

DEPARTMENT OF HOME AFFAIRS

DIRECTOR, CROSS-BORDER & CYBERCRIME SECTION

ELECTED COUNCIL OF EUROPE CYBERCRIME CONVENTION BUREAU MEMBER

About me

Admitted lawyer to the Supreme Court of New South Wales
Master's degree of Criminology and Criminal Justice
Double Bachelor's degree (Psychology/laws)
Graduate certificate in cyber law and investigations

Federal Prosecutor, human exploitation and cybercrime (2013-2015)
Electronic surveillance laws and policy officer (2015-2018)
Criminal justice and national security data access treaty negotiator (2018-current)

WHAT IS DIGITAL EVIDENCE?

- Begins as electronic data, either in the form of a transaction, a document, or some type of media (e.g. audio or video recordings.
- The reach of digital evidence – explosion of technology in our homes, our cars, social media, blogs, communications technology.
- Digital evidence is no longer localised on a person's devices – CLOUD storage, information logged with third party companies (such as communications occurring in chats).

More than 7.4 million images of child abuse circulating in Victoria

By Chris Vedelago
June 19, 2020 — 11.45pm

THE AGE

JACET said many parents were unaware that their children could be exposed to predators through Xbox and Playstation consoles that have text and audio chat functions.

NEWS

Snapchat predator groomed

Teenage killer confesses crime in World of Warcraft chat, sentenced to life in prison

bulk
by an

himself
hile she

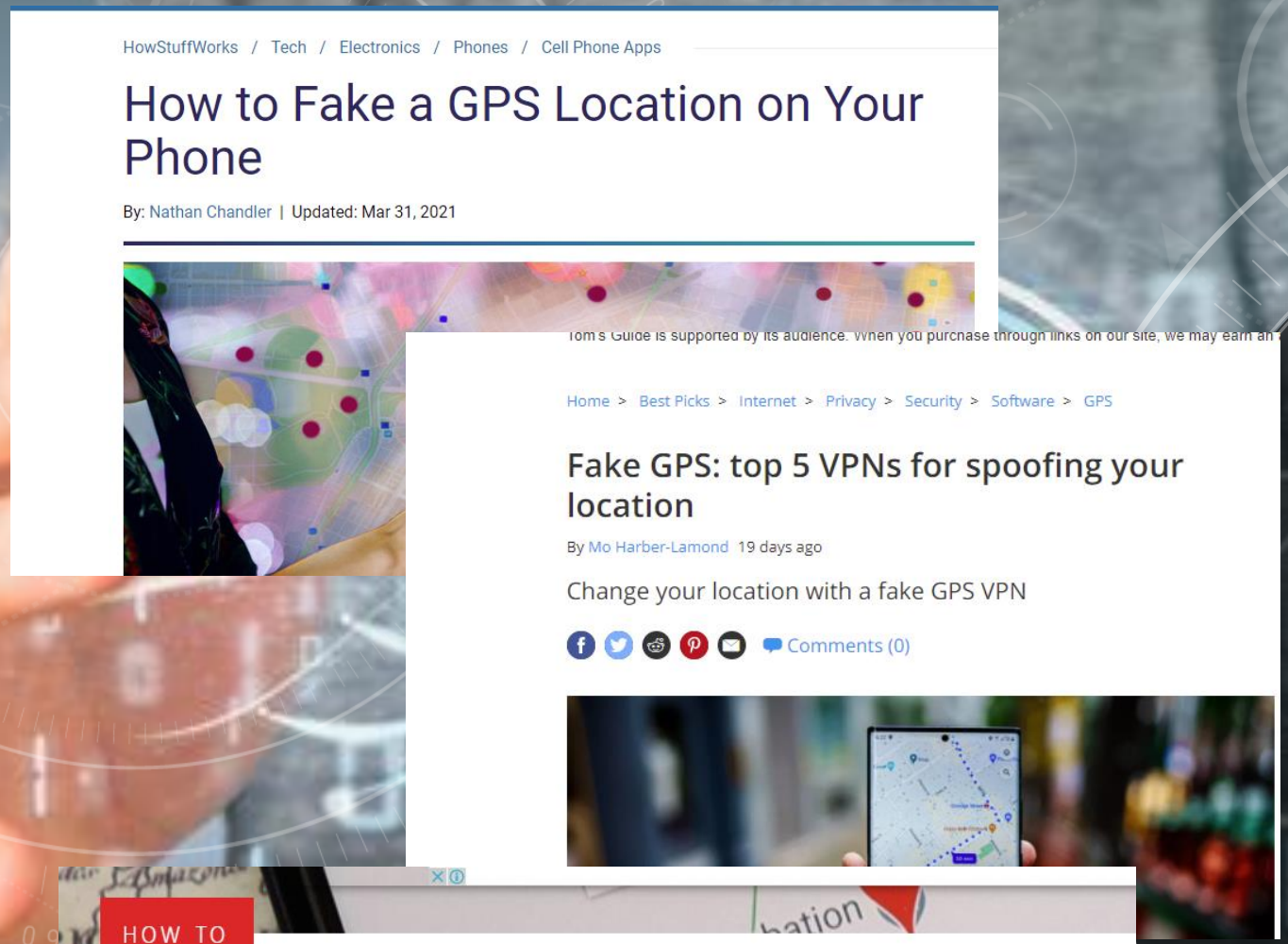
Pip Christmass • 7NEWS Published: Monday, 19 April 2021 6:58 pm AEST

Questions

Where is the digital evidence here?

How is it created?

In game chat functions



OTHER FORMS OF DIGITAL EVIDENCE

DIGITAL FOOTPRINTS – COOKIES!

INFORMATION ASSOCIATED WITH PRODUCED DIGITAL EVIDENCE

CHALLENGES – DIGITAL EVIDENCE

- Identification – Law enforcement technical identification capacity
- Not just whether digital evidence may exist, but
  - Where the evidence is stored,
  - Getting access to that storage,
  - Recovering and processing that digital evidence.
- Encryption and operational security measures
- Examples of law enforcement rising to these challenges

DEALING WITH DIGITAL EVIDENCE: A PROSECUTOR WISH LIST*

- Need to ensure that digital evidence is collected, preserved, examined.
- Afforded correct continuity procedures to safeguard challenges to the evidence.
- My four key principles:
  - Principle one – don't take any action that would change the data held on an electronic device or storage media which may be substantially relied upon for an investigation or prosecution.
  - Principle two – where it is necessary to access original data held on an electronic device or storage media, the relevant law enforcement officer should be adequately competent to deal with the device (including how and why).
  - Principle three – all processes applied to electronic devices should be documented.
  - Principle four – continuity!!

*These represent my own view based on experiences and may not be the official procedure or principles applied of the Australian law enforcement or prosecuting bodies.

DIGITAL EVIDENCE AND LEGAL FRAMEWORKS

- Digital evidence – What is the ultimate aim? Ordinarily a successful prosecution.
- Before digital evidence can be analysed, it must be identified and preserved: Criminal procedural laws need:
  - effective search and seizure warrant frameworks,
  - Assistance laws that allow for voluntary and compelled disclosure of third parties (such as electronic surveillance laws).
- Challenges in prosecuting criminal conduct on digital evidence
  - Ongoing development of various digital evidence analysis techniques (including penetration of devices),
  - Need for expert witnesses to describe the how and why? (complex for juries),
  - Admissibility – procedural frameworks and evidence laws to satisfactorily introduce digital evidence for both the prosecution and accused persons.

WHY INTERNATIONAL COOPERATION MATTERS

- We are not in this alone – Global problem.
- Increasingly digital evidence is held offshore – especially where this relates to cybercrime or where the internet is a facilitator.
- Forms of international cooperation –
  - Government-to-government (mutual assistance, law enforcement-to-law enforcement).
  - Government-to-private industry.
- Tips:
  - Law enforcement officers should be familiar with the common data-controller jurisdiction policies around international cooperation.
    - Example – Obtaining subscriber information from US providers directly without the need for a mutual assistance request (voluntary disclosure process).
  - Determine as early as possible whether a mutual assistance request, or direct requests, will be required.

INTERNATIONAL FRAMEWORKS – COUNCIL OF EUROPE BUDAPEST CONVENTION ON CYBERCRIME

- Australia is a signatory and has ratified the Budapest Convention on Cybercrime
- Provides a framework for the following:
  - (i) the criminalisation of conduct ranging from illegal access, data and systems interference to computer-related fraud and some child exploitation online (substantive criminal laws).
  - (ii) procedural law tools to investigate cybercrime and **secure digital evidence in relation to any crime**.
  - (iii) **efficient international crime cooperation**.
- There are current 65 members to the Budapest Convention, including major data controller countries such as the United States.
- Modernising the Budapest Convention – current negotiations for the Second Additional Protocol.
  - Enhanced and emergency international crime cooperation.
  - Joint investigations and investigative teams.
  - Direct disclosure of certain non-content data (such as subscriber information).
  - Many others!
- More than just a legal framework – A trusted community that permits hundreds of practitioners from Parties to share experience regularly and create relationships that facilitate international cooperation.

ANY QUESTIONS?