Module 7
(International Cybercrime Laws)

• At the end of this module you should have an appreciation for the cybercrime laws of a variety of foreign countries and appreciate the necessity of understanding them when performing a penetration test using resources outside the United States.
Canadian Cybercrime Laws

Criminal Code of Canada §184:
- Intercepting private communications using an “electro-magnetic, acoustic, mechanical or other device”
- Exception if originator consents to the interception, or if interception is necessary for maintaining quality of service, or to protect against some act under §342 or §430 (damage of property)
- Sentence not to exceed 5 years.

- Criminal Code of Canada §342: Offenses against rights of property
  - Forbids “faudulently and without colour of right” obtaining services, intercepting communications on a computer, trafficking in passwords.
  - Sentence up to 10 years.

- Criminal Code of Canada §402.2: Identity theft
  - Possession of identity information in circumstances giving rise to reasonable inference of intended use in commission of a crime.
  - Sentence not more than 5 years.

- Criminal Code of Canada §403: Identity fraud
  - Sentence of not more than 10 years.
UK Cybercrime Laws

• Computer Misuse Act of 1990
  – Guilty when
    • A person causes a computer to perform any function
      with intent to secure access to any program or data held
      in any computer
    • the access is unauthorized, and
    • The person knows at that time this is the case.
  – Unauthorized acts intended to impair (or with
    recklessness as to impairing) operation of
    computer.
  – Can be imprisoned up to 5 years.
German Cybercrime Laws

• German Criminal Code (GCC)§202a: Data Espionage
  – Outlaws obtaining data protected against access
  – Can lead to a 3 year prison term.

• German Criminal Code (GCC)§202b: Phishing?
  – Outlaws interception of communications

• German Criminal Code (GCC)§202c: Anti-Hacking Law
  – Outlaws preparing for an offense under 202a or 202b by producing, selling, supplying, or acquiring
    • Passwords or password finding tools
    • Software tools to commit such offenses
• German Criminal Code (GCC)§303a
  - Forbids unlawful erasure, suppression, rendering useless, or altering data. (2 year term.)
• German Criminal Code (GCC)§
  - Interfering with data processing operations to commit an offense under 303a, or to damage or destroy a data processing system can lead to up to a 5 year term
Australian Cybercrime Laws

- New laws took force on 1 March 2013. Updated to satisfy the Council of Europe Convention on Cybercrime.
- Requires carriers to preserve data communications.
- CyberCrime Act of 2001
  - Division 477: Outlaws unauthorized access, modification, or impairment of data and electronic communications with intent to commit a crime.
  - Division 478: Outlaws unauthorized access to data protected by an access control system or producing, supplying, or obtaining programs and data to commit an offense.
- Imprisonment of “5 or more years” can be for life.
Japanese Cyber Crime Laws

• Law No. 128 of 1999: Prohibition of acts of unauthorized computer access
  - Illegal to conduct or permit unauthorized computer access.
  - Illegal to evade access restrictions.
  - Cannot provide a person's authentication information to anyone unless you are the access administrator or at the administrator's request.
  - Not more than 1 year sentence and 500,000 ¥.

• These laws may be changing soon to satisfy the Council of Europe Cybercrime Convention