Cybercrime Statutes for Sydney, Australia

In recent years, the evolution of technology has placed an unprecedented burden on lawmakers of the world to adopt policies that handle a new and misunderstood medium of committing unlawful acts, cybercrime. In most countries, the politicians and lawmakers in power were raised in a world without the internet, which has made it difficult for them to define cybercrime in a uniform way, like we do with physical crime. Most jurisdictions agree that any violent act, such as assault or murder, are punishable offenses by law. These jurisdictions have written policies in place to specify how a physical crime is investigated, processed, and prosecuted. In cybercrime, many countries fail to agree on a uniform definition or procedures for processing such crimes. This paper discusses some measures taken by the government of Sydney, New South Wales, Australia to prevent, investigate, define, and prosecute cybercrime, as well as describes some situations these laws may apply towards.

First, the *Cybercrime Act of 2001* (Cth) sch 1(4) (Attorney-General's Department) (R v Boden)lays out exactly what constitutes as a cybercrime. This act prohibits any user from accessing data on a machine they do not have permission to access, altering any data to that machine, or causing the data to be unavailable to its intended user. The act states that the prosecution must have proof that the suspect intended to access the data, regardless of if the suspect knew it was illegal or not. To put it plainly, if an uneducated user accidentally stumbles upon another user’s data, they would not be held liable to the criminal act of accessing that data. The offense carries a maximum sentence of 10 years in prison. This may cause problems for a pen-tester, because they will be granted access to some parts of the machine but restricted from the others. If a

pen-tester overreaches their boundaries and goes through the file system unauthorized, they may be held legally responsible. Because of this, the pen-tester must be cautiously aware of what data on the machine is authorized by the client to be looked at. There is a case from 2002 that dealt with this law. In *R v Boden* (2002), a disgruntled ex-employee, Votek Boden, hacked into the computer systems that at the Maroochy Shire Council's sewer system. This sewer system was installed by Hunter Watertech, a company in which Boden had resigned from a few years prior. Boden had requested to be re-employed by Hunter Watertech, a request that was denied by the company. According to the case, Boden had stolen a private two-way radio to send communications to sewage pumping stations and caused them to malfunction. This resulted in sewage polluting 500 meters of nearby water supplies and killing marine life. He was charged with 26 counts of misusing a computer without the permission of its legal owner, and various other charges related to the events that ensued due to his actions. (R v Boden) Not only should a pen-tester be aware of the laws regarding their job, but companies must also consider the risk that an ex-employee poses to the company. Any previous access must be revoked and tested to ensure another event like this one doesn't happen again.

However, an irresponsible pen-tester may also be prosecuted for acts that have little to do with computer or cybercrime laws. If data is destructed in negligence from the investigator, they may be charged with destroying or damaging property, detailed in the *Crimes Act 1900* s 195 (New South Wales Government) This section in the Crimes Act of 1900 says that any destruction of private property, whether intentional or reckless, may face up to 5 years in prison. A pen-tester's job can involve working on volatile

hardware and data, so they must be cautious and aware of every action they do and its consequences. It would be a good practice for an investigator to work solely on a bit for bit copy of the system, so that if any data is corrupted, it can be restored.

Now that federal and state laws have been covered, it's now time to take a look at any local or citywide laws that may impact a penetration testing investigation. In Sydney, there aren't many (if any) laws on the municipal level regarding computer crimes that aren't covered by the laws in the higher tiers of government. If a pen-tester is hired to conduct a test in Sydney, they should follow the laws at both the federal and state levels.

To summarize, it is detrimental for a cyber security professional to ensure they understand what laws are in place, to avoid any litigation or criminal charges. The professional must keep a close eye on every action completed in an investigation. If unsure, the investigator should consult law enforcement or the government legislature website. It also would be a good idea to get a robust contract form the client that specifies what authorization will be granted to the investigator. This way, if the client suffers from any loss due to the process of the investigation, the investigator is covered legally and in writing as long as they follow the clearly defined boundaries. Any ambiguity in a contract may lead to the investigator being held liable for damages incurred.

Bibliography

Attorney-General's Department. "Cybercrime Act of 2001." 01 October 2001. *Australian Government Federal Register of Leglislation.* 19 September 2021. <https://www.legislation.gov.au/Details/C2004C01213>.

New South Wales Government. "Crimes Act 1900." Vers. 195. 27 March 2021. *NSW Legistlation.* 18 September 2021. <https://legislation.nsw.gov.au/view/html/inforce/current/act-1900-040#pt.4AD-div.2>.

R v Boden. No. 164. Queensland Court of Appeals. 10 May 2002.