TECHNOLOGICALLY-FACILITATED VIOLENCE:
UNAUTHORIZED USE OF A COMPUTER

A. OFFENCE ELEMENTS 2

B. SELECTED CASE LAW 3

I. SUPREME COURT OF CANADA 3
i. 2012 SCC 53 3
II. ALBERTA 4
i. 2013 ABPC 116 4
III. NOVA SCOTIA 6
i. 2010 NSSC 253 6

A. OFFENCE ELEMENTS

Unauthorized use of a computer

342.1(1) Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service;

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).

B. SELECTED CASE LAW

I. SUPREME COURT OF CANADA

i. 2012 SCC 53

In **2012 SCC 53**, during routine maintenance on a high-school teacher's employee laptop a technician found sexually explicit nude images of a grade 10 girl on a hidden folder on the hard drive of the computer. The teacher, Mr. C, had access to all of the student's school laptops and had copied the pictures from a student's laptop onto his workplace laptop. After discovering the images, the technician reported the images to the principal, who instructed the technician to copy the images onto a compact disc. The school then seized the laptop and had the technician's copy the temporary internet files onto a second compact disc. The police were contacted, who seized the computer and CDs, and made a mirror image of the hard drive for forensic purposes. Mr. C was charged with possessing child pornography and the unauthorized use of a computer, however, Mr. C argued that the evidence should be excluded because the police had violated his section 8 Charter right to be protected from unreasonable search and seizure when the police seized and searched the CDs and laptop without a warrant.

At the trial level, 2008 ONCJ 278, the judge found that Mr. C's section 8 Charter rights were infringed and excluded all of the computer material pursuant to section 24(2) of the Charter. The appeal court, [2009] 190 CRR (2d) 130 (ONSC), did not find a section 8 breach and reversed the decision of the trial judge. The Court of Appeal, 2011 ONCA 2018, set aside the decision of the appeal court and excluded the CD with the temporary internet files, the laptop and the mirror image of the hard drive. The Supreme Court held that Mr. C did have a reasonable expectation of privacy in his work computer because it contained information that was meaningful, intimate and touching on the user's biographical core. The school board's workplace policies and practices were found to diminish his expectation of privacy on the

device, but not remove it completely. Mr. C's employer had lawful authority to seize and search the laptop but could not provide third party consent for the police to search the laptop, even though the device and the data contained on it were property of the schoolboard. In failing to obtain a warrant prior to searching the laptop, the police infringed Mr. C's rights against unreasonable search and seizure. The CD containing the photos were not disputed as admissible evidence, however, the Court held that admitting the other disputed evidence would not bring justice into disrepute and did not exclude the evidence from the second CD, laptop or mirror image of the hard drive.

II. ALBERTA

i. 2013 ABPC 116

In **2013 ABPC 116**, Mr. M, a security guard in his twenties, pleaded guilty to 39 criminal charges against 21 child victims over a five-year period. Charges included multiple counts of internet luring, extortion, child pornography offences, invitation to sexual touching, identity fraud, unauthorized use of computer with intent to commit mischief in relation to data, and failure to comply with recognizance which prohibited his contact with a person under the age of 18 without supervision and prohibited Mr. M's use of the internet.

Over a five-year period, Mr. M used Facebook, Nexopia, and other messaging programs to contact children and request photographs of them in their underwear or in the nude, and/or for them to expose themselves or engage in sexual behaviour on webcam. He also communicated with children—the majority of whom were boys and girls between the ages of 11 and 16—using MSN Messenger and through text messages. If his victims refused to send him nude photographs, Mr. M would use information he had learned about the children in past conversations to hack into their email and social media accounts (for example, by asking questions related to common password reset security questions such as pet names and

birthdays) and threaten them. On more than one occasion, M impersonated his child victims in order to solicit nude photographs from their friends. In other instances, after hijacking his victims' online accounts, he told children they could only regain access to their accounts if they sent him nude photographs. When one child sent Mr. M photos of her in her underwear, he threatened to distribute the photos unless she sent him a fully nude photograph. He also sent explicit photos to some victims. Mr. M also distributed photos of his victims on the internet. If he had copies of photographs of the children in their underwear or in the nude, he would occasionally post those pictures on the child's social media or upload them as the child's profile picture in order to extort more pictures. In some conversations, he requested the children to touch themselves sexually and have sexually explicit conversations with him. Mr. M also altered photos to appear as though the child was naked. Several parents reported his behaviour to the police and to the social media companies, some of whom alerted the police of the problematic behaviour.

At sentencing, the Court noted that Mr. M's actions were deliberate, persistent, and aggressive. The offences were also sexually motivated, and the Court found that they were "calculated to intimidate, manipulate and psychologically and socially harm the vulnerable child and youthful victims." The only mitigating factors on sentencing were the facts that Mr. M pleaded guilty to all charges and had cooperated with police.

The Court considered some of Mr. M's conduct "cyberbullying," and cited *AB v Bragg Communications* 2012 SCC 46 to describe the harm that cyberbullying can do to children. The Court noted that "[Mr. M's] use of the internet, to commit his numerous sexually based criminal offences involving children and young adults, have elements of disturbing online sexual harassment - an adult criminally cyberbullying and cyberstalking, calculated to randomly choose youthful victims to emotionally harass, threaten, intimidate and manipulate in furtherance of his criminal objectives." Mr. M was sentenced to 11-years imprisonment, along with several ancillary orders including prohibitions on possession of firearms and limitations on attending

places where persons under 16 are present, prohibiting him from being in a position of authority with persons under the age of 16, an order to provide a DNA sample, and an order to comply with the Sexual Offender Information Registry Act.

III. NOVA SCOTIA

i. 2010 NSSC 253

In **2010 NSSC 253**, Mr. S was charged with unlawfully using a computer to communicate with a person believed to be under the age of 14 for the criminal purpose of luring a child and inviting the child to sexual touching. He was also charged with unlawfully obtaining a computer service without a colour of right by accessing his neighbour's wifi without consent. An undercover police officer acting as a 13-year-old boy began communicating with Mr. S in a teen chatroom where Mr. S sent sexually explicit messages and images and encouraged the boy to touch himself sexually. After his arrest, Mr. S claimed that he believed he was role playing with another adult man pretending to be an underage boy and argued he thought he was using the wifi from his landlord's router in his building. He was found guilty of unlawfully using a computer to commit offences against the child, but was acquitted of the unlawful use of his neighbour's wifi.