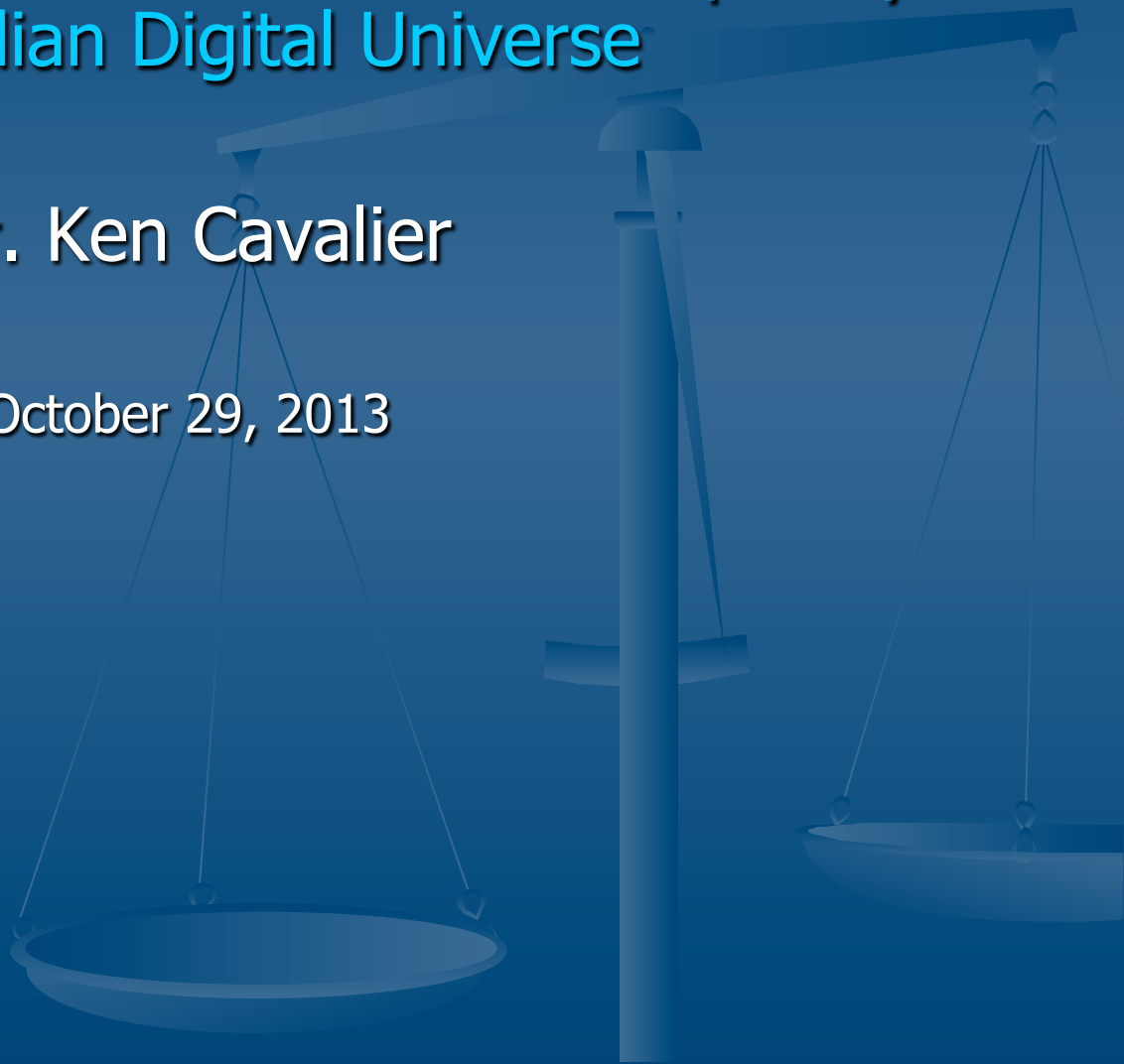
Crime and Punishment in The Contemporary Canadian Digital Universe

Dr. Ken Cavalier

October 29, 2013



Law as a Dispute Resolution Mechanism for Legal Relationships

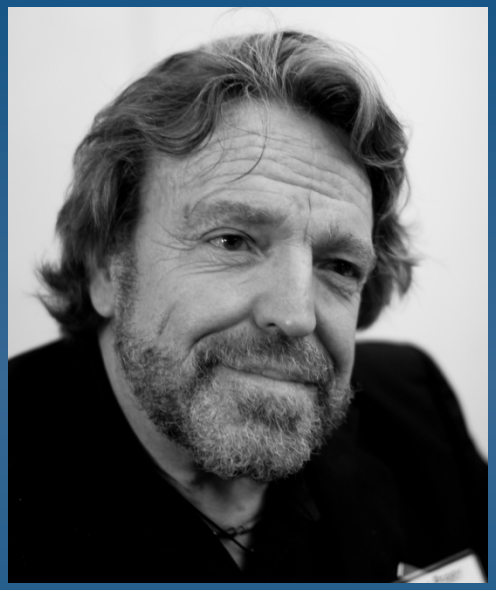
Introduction

- The Purposes of Law
- Punishment and Deterrence
- Crimes and Regulation
- Legal “Wrongs” or Torts
- Restitution

Jurisdiction and Burden of Proof

- **Borders Matter even in Cyberspace**
- **Plaintiffs Bear the Burden of Proof of the Tort or Legal Wrong**
- **The Standard of Proof for Torts is on the Balance of Probabilities**
- **Plaintiffs have a duty in Torts to Mitigate their Damages**
- **In Criminal Law disputes, the State Bears the Burden of Proof Against the Defendant**
- **The Standard of Proof for Criminal Liability is Beyond A Reasonable Doubt (BARD)**

John Perry Barlow



- Lyricist for the Grateful Dead
- Co-Founder of the Electronic Frontier Foundation and Reddit
- Cyberspace Activist and Fellow at Harvard University's Berkman Center for the Internet and Society.
- Wrote "A Declaration of the Independence of Cyberspace" http://anoninsiders.net/cyberspace-independence-declaration-694/ February 8, 1996
- Inducted into the Internet Hall of Fame

Criminal Code of Canada Provisions

- S. 46 in Part II Offenses against Public Order describes Treason in Canada that could come with a 14 year sentence or a life sentence if Canada is in a state of war
- Issues of Invasion of Privacy are dealt with in the Criminal Code beginning in s. 183 Part VI
- **184.** (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

S. 184 Interception of Private Communications

Interception

- **184.** (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

- …Saving provision

- (2) Subsection (1) does not apply to

(e) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for

(i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or

(ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1).

S.191 Devices enabling the Interception of Private Communications

- Offences concerning the possession and forfeiture of devices enabling the interception of Private Communications are dealt with in s. 191
- **191.** (1) Every one who possesses, sells or purchases any electro-magnetic, acoustic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communications is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

S. 342.1 **Unauthorized use of computer**

- **342.1** (1) Every one 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 an offence under section 430 in relation to 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*)
- is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

S. 342.2
Possession of device to obtain computer service

- **342.2** (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,
  - (*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
  - (*b*) is guilty of an offence punishable on summary conviction.

Computer Fraud and Identity Theft

- **Identity theft**
- **402.2** (1) Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.
- **Trafficking in identity information**
- (2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

s. 402.2 Identity Theft

- Punishment
- (5) Everyone who commits an offence under subsection (1) or (2)
- (a) is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or
- (b) is guilty of an offence punishable on summary conviction.
- 2009, c. 28, s. 10.

S. 430 Mischief

- **430.** (1) Every one commits mischief who willfully
- (*a*) destroys or damages property;
- (*b*) renders property dangerous, useless, inoperative or ineffective;
- (*c*) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
- (*d*) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.
- **Mischief in relation to data**
- (1.1) Every one commits mischief who willfully
- (*a*) destroys or alters data;
- (*b*) renders data meaningless, useless or ineffective;
- (*c*) obstructs, interrupts or interferes with the lawful use of data; or
- (*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Mischief is Serious

- **Punishment**
- (2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.
- (3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five thousand dollars
- (*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
- (*b*) is guilty of an offence punishable on summary conviction.
- **Idem**
- (4) Every one who commits mischief in relation to property, other than property described in subsection (3),
- (*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
- (*b*) is guilty of an offence punishable on summary conviction.

IP Restrictions of Expression

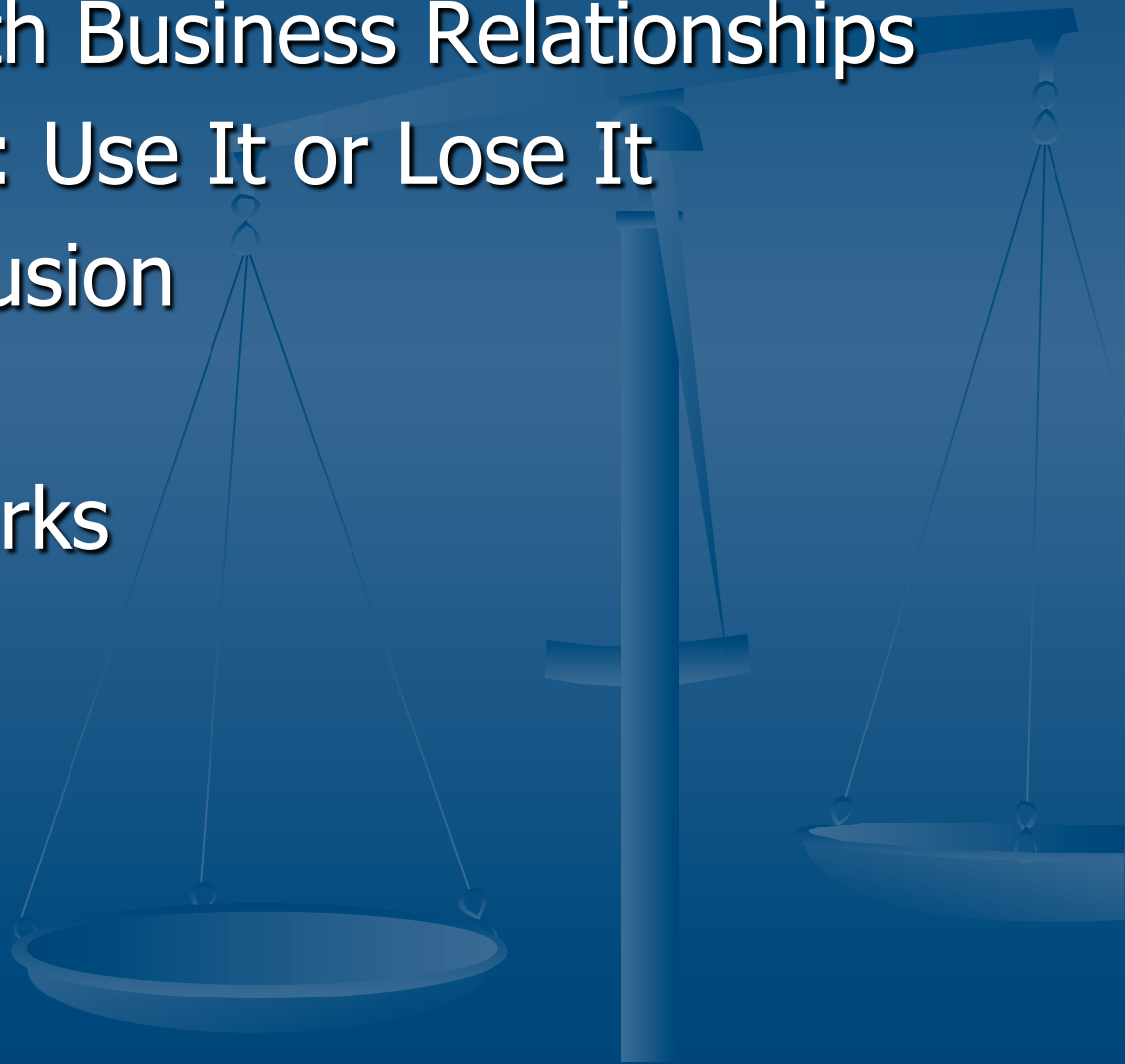
- Copyright Act prohibits unauthorized copying and derivative works usually for life of the author plus 50 years.
- Patent Act grants exclusive right to economically exploit innovative invention but only allows improvement patents with patent holder's permission for 20 year period

Copyright Modernization Act. R.S., c. C-42

- Passed in 2013 in response to Canada's International Obligations under the WIPO Copyright Treaty that Canada had signed but been unable to ratify domestically
- Acknowledges "User Rights" but includes Rights Owner Protection for TMP and ARM systems
- Broadens Fair Dealing Provisions to include parody and educational use
- Obligates fair dealer to destroy copies after educational use

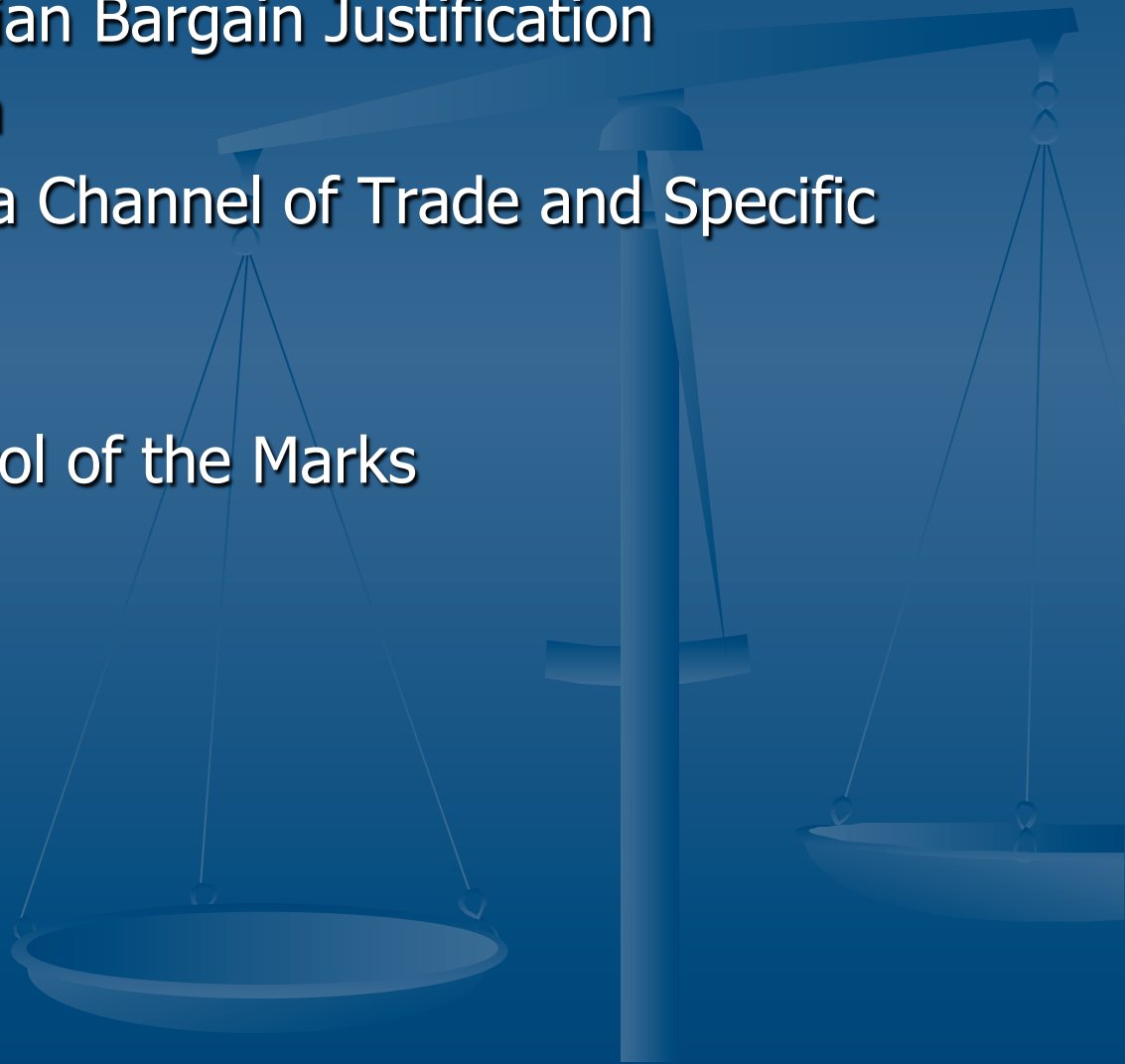
The Trade Marks Act and Unfair Business Practices

- Interference with Business Relationships
- Trademark Law: Use It or Lose It
- Consumer Confusion
- Passing Off
- Control over Marks
- Dilution



Overview of Canadian Trademark Law

- Common Law Utilitarian Bargain Justification
- “First to Use” system
- Trademark “Use” in a Channel of Trade and Specific Jurisdiction
- Use it or Lose it
- Ownership and Control of the Marks



Canadian Trademark Case Law Constitutional Challenge Concerns

Division of Powers

MacDonald v. Vapor Canada Ltd. 1976

Declared s. 7(e) TMA prohibition against any business practice contrary to honest industrial or commercial usage in Canada *Ultra Vires* due to competing provincial jurisdiction and "vagueness"

Freedom of Expression and "Ambush Marketing"

National Hockey League v. Pepsi-Cola Ltd. 1992

Ambush marketing properly done does not constitute trademark infringement

Other Canadian Trademark Law Concerns

Grey Marketing or Parallel Importing

Smith & Nephew v.Glen Oak Inc., (1996),

Legal in Canada

The "Public Authority" Status of the C.O.C. and VANOC

See You In Athletics Fund v. Canadian Olympics Committee (2007)

The C.O.A. is a "public authority" in Canada.

Reputational Rights and Other Torts

- On-Line Defamation
- Product Libel
- Interference with Contractual Relations
- Tarnishment

Espionage Statutes and National Security

- *Security of Information Act*. R.S.C., 1985, c. O-5, s. 1; 2001, c. 41, s. 25. (Formerly the Official Secrets Act) Canada
- U.S. Espionage Act (1917) 18 U.S.C. ch. 37 (18 U.S.C. § 792 et seq.) U.S.
- U.K. Official Secrets Act (1989) , ch. 6, 1989, http://www.legislation.gov.uk/ukpga/1989/6/contents

- Seumas Milne

SPYING BY THE GOVERNMENT

GCHQ UK.

Intelligence Services Act (1994), ch. 13.

http://www.legislation.gov.uk/ukpga/1994/13/contents

NSA Agencies U.S.

Patriot Act and *Prism* program

Canada has is own CSIS

- *Canadian Security Intelligence Service Act*.
- 1984, c. 21, s. 1.

Famous Whistleblowers and the Culture of Leaks of Confidential Information

- Daniel Ellsberg released the Pentagon Papers (1971) to the New York Times
- Release led to (*New York Times Co. v. United States*). Appellate decision.
- Leaked to Washington Post and 17 other papers when injunction against New York Times was granted
- Anti-war activist, both Viet Nam and Iraq
- Supporter of Snowden
- Economist in the field of "decision theory"
- Detailed the Ellsberg paradox in decision making

“Ethical Hackers” or Reckless Endangerers?

- Edward Snowden NSA Contractor
- Samuel A Adams “whistleblower” Award
- Charged with Espionage
- Has claimed Asylum in Russia
- Revelations about US spying on allied foreign leaders has led to diplomatic crisis and heightened privacy concerns

Chelsea (Bradley) Manning

Received 35 year sentence (with possibility of parole in 8 years) and dishonourable discharge under U.S. Espionage Act and Computer Fraud and Abuse Act ((18 U.S.C. § 1030) for Wikileaks disclosure of classified U.S. documents relating to Iraq War.
Has since undergone gender reassignment and become Chelsea

Julian Assange and Wikileaks

- Mendax “nobly untruthful” and Nortel Hacking at 17
- The *Personal Democracy Forum* said he was "Australia's most famous ethical computer hacker".
- Samuel A Adams “whistleblower” Award
- Sought Asylum in Ecuadorian Embassy in London
- 30 November 2010, Canadian Tom Flanagan, former Harper Aide called for Assange’s assassination, which he later retracted
- Subject of The Fifth Estate bio-pic
- Charged with sexual misconduct while in Sweden
- Released 251,000 US government cables, many of which were unredacted, allegedly putting sources at risk

Jeffery Delisle Canadian Naval Officer --Traitor

- On February 8, 2013 Delisle was sentenced to 20 years in prison and fined nearly $112,000.
- On February 13, 2013 it was announced by DND that Delisle had been stripped of his commission and service decorations and been dishonourably discharged.
- DND was also moving immediately to recover the salary paid to Delisle since his arrest in January 2012
- 23 payments amounting to $71,817 over nearly five years, beginning in 2007.

Conclusions: Concerns

- How can the Law balance competing rights such as Freedom of Expression with Privacy Rights?
- How can the Law balance competing rights such as The Freedom of the Press with Privacy Rights and National Security?
- How can the Law balance competing rights to anonymity and the right to be forgotten with protection of reputational rights?
- How can the Law balance competing rights such as Transparency in Government with Protection of Privacy Guarantees? (FOI and PIP)

Martyr In the Struggle for Open Source

- **Aaron Hillel Swartz**
- **Downloaded JSTOR academic articles and charged with wire fraud and 11 violations of the Computer Fraud and Abuse Act**
- **Committed suicide January 11, 2013**
- In June 2013, Swartz was posthumously inducted into the Internet Hall of Fame.

Conclusion

Law has traditionally been based upon an adversarial system of adjudicating competing claims. More recently alternative dispute resolution methods have been encouraged to level the playing field among the participants. That being said, given the stresses of litigation and legal defence, we must recognize there exists an imbalance of power between the individual and the legal system, especially in criminal law. Individual rights to due process and equity must be encouraged for just results. Laws impose obligations upon those who enter into legal relationships with other individuals or groups or the state. Some of those obligations may seem onerous, but the maintenance of the legal system and the rule of law is a result worth fighting for, especially in cyberspace. The management of the new knowledge economy based as it is on more and more intangible property and needing to accommodate notions of collective ownership and non-rivalrous ownership. In the digital environment older notions of what constitutes admissible evidence, or the best evidence, verification of the chain of custody of electronic documents through the careful recording of metadata associated with them and other issues of access and control of digital documents ensure that the practice of law will have to change. Questions of ISP and hosting liability, regulation of the Internet, the effect of Big Data and Protection of Privacy concerns will keep changing the legal landscape and liability of users of computers for years to come.

Thank you