

CompSci 725

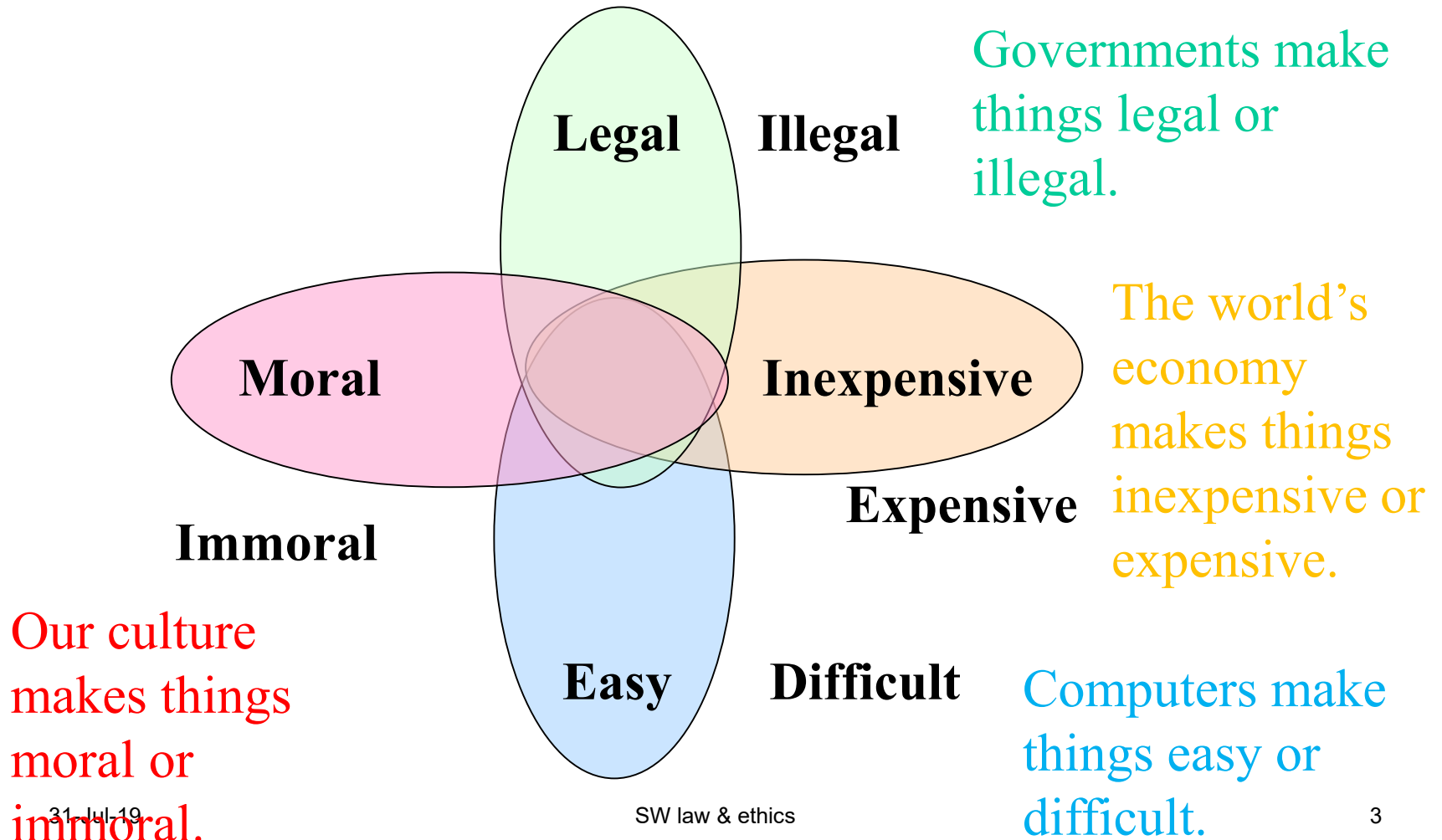
“Soft” Security

Clark Thomborson
University of Auckland

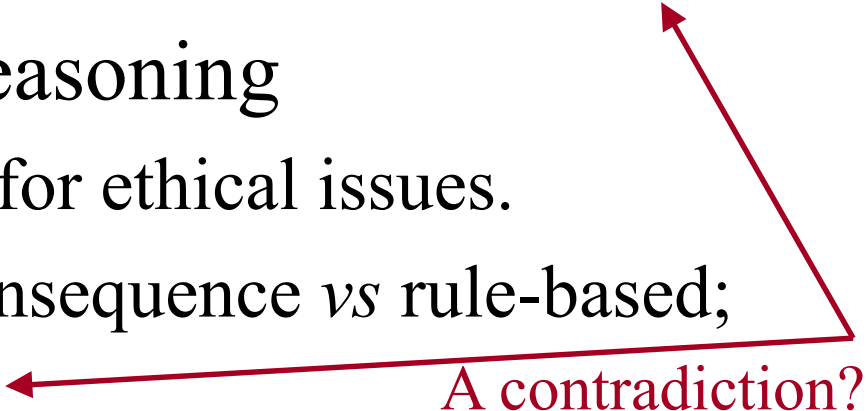
Real-World Security Analysis

- *Whose* security is being protected?
 - Every person, and every organised group of people, has security objectives.
 - No computer has security objectives. (Do you agree?)
- *How* could the secured entity be harmed?
 - “Security objective” e.g. loss of an asset
- *Who* might want to harm this entity?
 - “Threat agent”, “threat model”
 - (How can a threat model be validated? Can it be verified?)
- Is the control *proactive* (with guards), or *reactive* (with judges)?
- Is the control *hierarchical*, or is it *democratic*?
 - Hierarchs control their organisation by administering threats and rewards. (A rule of law, or an arbitrary ruler? Do you have multiple rulers?)
 - Peers control their society by shaming, persuading, gossiping, buying and selling. (Do you live in a single society, or are your ethical controls context-dependent?)

Lessig's Taxonomy of Control



Ethics for IT Security (Pfleeger, 1997)

- What is ethics?
 - “Through **choices**, each person defines a **personal set** of ethical practices [when deciding right actions from wrong actions].”
 - Ethics is not law, not religion, and not universal.
 - Principles of Ethical Reasoning
 - How to examine a case for ethical issues.
 - Taxonomy of ethics: consequence *vs* rule-based; individual *vs* universal. 
- ☞ You make choices every minute, are all your choices ethical?

Universal, Rule-Based Ethics

- Pfleeger suggests the following “basic moral principles” are “universal, self-evident, natural rules”:
 - The right to know
 - The right to privacy
 - The right to fair compensation for work
- ☞ Should you expect users to obey these rules, when you are designing a security system?
- ☞ Should you enforce these rules in your systems?

Our Duties, from Sir David Ross

- Fidelity (truthfulness)
 - Reparation (compensate for wrongful acts)
 - Gratitude (thankfulness for kind acts)
 - Justice (distribute happiness by merit)
 - Beneficence (help other people)
 - Nonmaleficence (don't hurt other people)
 - Self-improvement (both mentally and morally, *e.g.* learn from your mistakes)
- ☞ Which of these duties support our “rights” to knowledge, privacy and compensation?
- ☞ Are these universal duties, or merely “Western/Christian”?

Christian Ethics, in brief (Huston Smith, 1989)

- Moses: don't murder, commit adultery, steal, lie.
 - New Testament: faith, hope, love, charity.
 - Golden Rule: “Do unto others as you would have them do unto you.”
- ☞ Which of these ethics support our “rights” to knowledge, privacy and compensation?

Confucian Ethics, in brief

孔夫子
Kǒng fū zǐ

仁
Rén
Ren (human-heartedness): “Measure the feelings of others by your own.”

義
Yì
Yi = zhong + shu (right conduct = doing one’s best + altruism): “How can I accommodate you?” not “What can I get from you?”

禮
Lǐ
Li (propriety): follow Confucius’ example, nothing in excess, respect for elders, ...

德
De (power of moral example): leaders must show good character.

文
Wen (the arts of peace): music, poetry, painting; contrast with the arts of war and commerce.

忠恕
Zhōng shù

己所不欲，勿施於人
Yourself, what [you] don't want, don't do to others.

Analects 15:23

Which of these ethics support our “rights” to knowledge, privacy and compensation?

Islamic Ethics, in brief

- Economic: don't charge interest (but you may invest for a share of profit); all offspring should inherit; 2.5% to charity each year.
 - Social: racial equality, no infanticide, women must consent to marriage.
 - Military: punish wrongdoers to the full extent of injury done; honour all agreements; no mutilation of wounded.
 - Religious: “Let there be no compulsion in religion.” (2:257)
- ☞ Which of these ethics support our “rights” to knowledge, privacy and compensation?

Individualism

- “God helps those who help themselves”
- Dale Carnegie: *How to Win Friends and Influence People*, 1936:
 - “Twelve Things This Book Will Do For You
 1. Get you out of a mental rut, give you new thoughts, new visions, new ambitions...
 4. Help you to win people to your way of thinking...
 7. Increase your earning power.
 8. Make you a better salesman, a better executive...”
- “Greed is good: A 300-year History of a Dangerous Idea”, The Atlantic, 7 April 2014.

Individualism in the Chinese Tradition

- “Unlike individualism in modern European and American contexts, Chinese manifestations of “individualism” do not stress an individual’s
 - separation,
 - total independence, and
 - uniqueness from external authorities of power.
- “Rather, individualism in the Chinese tradition emphasizes
 - one’s power from within the context of one’s connection and unity (or harmony) with external authorities of power.
- “... the Western tradition tends to view the individual in an atomized, disconnected manner, whereas the Chinese tradition focuses on the individual as a vitally integrated element within a larger familial, social, political, and cosmic whole.”

[Erica Brindley, Internet Encyclopedia of Philosophy, ISSN 2161-0002, retrieved 10 August 2017]

Ethical Communism

- “Nothing in society will belong to anyone,
 - either as a personal possession or as capital goods,
 - except the things for which the person has immediate use, for either his needs, his pleasures, or his daily work.
- “Every citizen will be a public man,
 - sustained by, supported by, and occupied at the public expense.
- “Every citizen will make his particular contribution
 - to the activities of the community according to his capacity, his talent and his age;
 - it is on this basis that his duties will be determined, in conformity with the distributive laws.”

[E-G Morelli, *Code of Nature Or, The True Spirit of Laws*, 1755. Trans. A Fried and R Sanders, ed., *Socialist Thought: A Documentary History*, Columbia University Press, 1964]

Cybernetics

- “Although Wiener [1954] stated his ‘great principles’,
 - he did not assign names to them.
 - For purposes of easy reference, let us call them ...
- **The Principle of Freedom**
 - Justice requires ‘the liberty of each human being to develop in his freedom the full measure of the human possibilities embodied in him.’
- **The Principle of Equality**
 - Justice requires ‘the equality by which what is just for A and B remains just when the positions of A and B are interchanged.’
- **The Principle of Benevolence**
 - Justice requires ‘a good will between man and man that knows no limits short of those of humanity itself.’

<https://plato.stanford.edu/entries/ethics-computer/>, retrieved 10 Aug 2017.

Some Simple Ethical Analyses

- “Might makes right” (i.e. legal \equiv ethical)? Or...
 - Does a society have a right to rebel against an unjust ruler?
 - Could an employee have an ethical obligation to refuse some work assignment, or to reveal some corporate secret?
- “Money is the root of all good” (i.e. economic \equiv ethical)
 - “Until and unless you discover that money is the root of all good, you ask for your own destruction.
 - “When money ceases to become the means by which men deal with one another, then men become the tools of other men.
 - “Blood, whips and guns or dollars. Take your choice - there is no other.” [Ayn Rand, *Atlas Shrugged*, 1957]
- “The love of money is a root of all kinds of evil, for which some have strayed from the faith in their greediness, and pierced themselves through with many sorrows” (i.e. economic \neq ethical) [I Timothy 6:10].

Utopian Ethics

- “A utopia is an imagined community or society that possesses
 - highly desirable or nearly perfect qualities for its citizens.
- “Utopian ideals often place emphasis on
 - egalitarian principles of equality in economics, government and justice, though by no means exclusively, with the
 - method and structure of proposed implementation varying based on ideology.
- “According to Lyman Tower Sargent ‘there are
 - socialist, capitalist, monarchical, democratic, anarchist, ecological, feminist, patriarchal, egalitarian, hierarchical, racist, left-wing, right-wing, reformist, free love, nuclear family, extended family, gay, lesbian, and many more utopias’.”

[<https://en.wikipedia.org/wiki/Utopia>, 10 Aug 2017]

Professional Ethics

- If you, as a computer professional, design a webservice for “real world security” as defined by Lampson,
 - Might your service be ethically offensive in some societies?
 - How can you design for all possible stakeholders? (“What do we want from secure computer systems?”)
- You might design a system that upholds Wiener’s “great principles” of freedom, equality, and benevolence.
 - Would that be enough to satisfy all of your stakeholders?
 - Might some stakeholders require your system to enforce an inequality?

Professional Codes of Ethics

- Most professional organisations, such as the IEEE, the ACM, and the RSNZ, have codes of ethics.
- If you transgress a professional code of ethics, your organisation may revoke your membership.
- To explore these ideas:
 - Examine the IEEE Code of Ethics. Is it congruent with Confucian ethics? With cybernetics? Explain.
 - Examine the RSNZ Code of Professional Standards and Ethics. Is it in conflict with the IEEE Code of Ethics? Explain.
 - Describe the “Ten Commandments of Computer Ethics” using Pfleeger’s terminology.

Individual Morality vs Ethics

- I believe security engineers have a moral obligation to minimize all foreseeable harm to legitimate stakeholders.
- What is your moral position on this aspect of professional ethics?

Using Ethics in System Design

- A thorough security analysis will consider the ethics of important stakeholders and of potent attackers.
 - Ethics will affect motivation, for good and for evil.
- A cost-effective system design will make assumptions about the ethics of its stakeholders.
 - Ethics will affect system uses and misuses.
- Because ethics are personal, and conditioned by our cultures, our ethical assumptions will be at least somewhat biased and inaccurate.
 - This is another reason why real-world security is imperfect.

Copyright, in Pfleeger's Ethics

- Samuel Johnson: “For the general good of the world,” a writer’s work “should be understood as belonging to the publick.” To which of Pfleeger’s “rights” does this argument refer?
 - ☞ The public’s right to information.
- Richard Aston: it is “against natural reason and moral rectitude” that a government should “strip businesses of their property after fourteen years.”
 - ☞ The publisher’s right to compensation.

Chinese Ethics of Copyright?

- In 1993, John Perry Barlow (noted cyberlibertarian) and Mitch Kapor (author of Lotus 1-2-3) visited a Hong Kong shop that specialised in “pirated” software.
 - Barlow saw “not the slightest trace of moral anxiety” in the salesclerk’s face, when Kapor informed her that he was the author of the work he was trying to purchase.
 - She said, “Yeah, but you still want a copy, right?”
 - [Charles C Mann, “Who Will Own Your Next Good Idea”, *The Atlantic Monthly*, September 1998.]
- What is “fair compensation for work”?
 - Employers might pay USD \$0.50/hour for Chinese labour, and USD \$10.00/hour here. Should copyright items cost 20x more in NZ than in China?
 - Confucian ethic of “Wen”: Mandarins should produce art but never sell it.
 - What were Mao’s thoughts on copyright?

Rosner's Ethics of Software Piracy

- “Steal this Software”, by Hillary Rosner, *The Industry Standard*, 26 June 2000:
 - “Insider’s entitlement”: if you’re clever enough to find “warez” then you deserve to have it without paying.
 - “If you buy any software, then you’re also in danger of buying the [Brooklyn] bridge if someone tried to sell it to you.”
- Was (is) this an accurate description of cracker (phreak) culture?

Rudimentary Treatise on the Construction of Locks, 1853

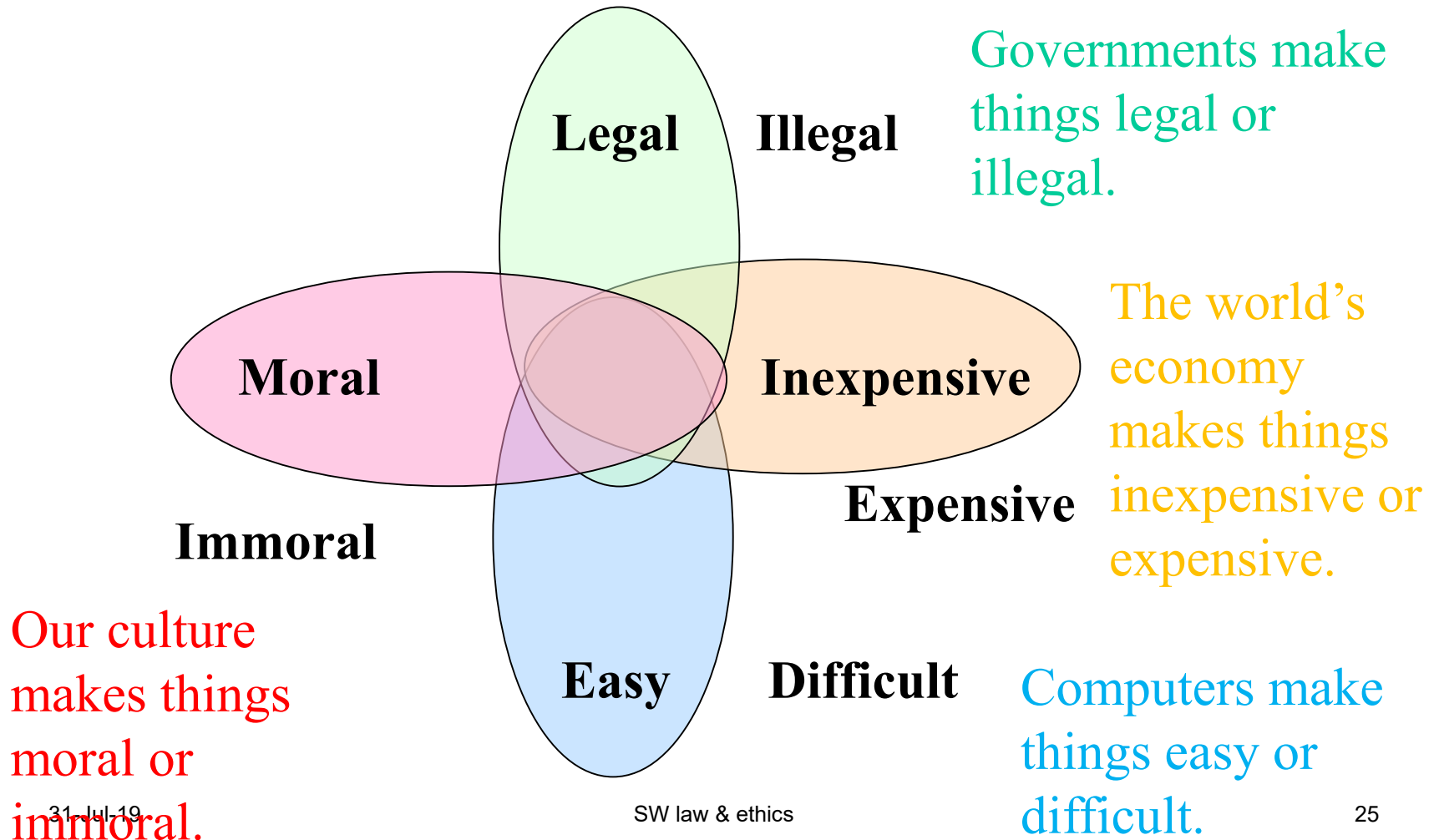
Charles Tomlinson

- “Rogues knew a good deal about lockpicking long before locksmiths discussed it among themselves.”
- “If a lock... is not so inviolable as it has hitherto been deemed to be, surely it is in the interest of *honest* persons to know this fact.”

Tomlinson's Argument (cont.)

- “The inventor produces a lock which he honestly thinks will possess such and such qualities; and he declares the belief to the world. If others differ... the discussion, truthfully conducted, must lead to public advantage.”
- What is your ethical analysis? (Right to information *vs* ??)
- Would your analysis change if the “lock design” were protected by trade secret?

Lessig's Taxonomy of Control



An Overview of “Software Law”

- There are many types of legal controls on your activities:
 - Certain actions (theft, fraud) are **crimes**.
 - A few actions (e.g. a “duty of care”) are **obligations**: you can be punished if you don’t do them adequately.
- Every jurisdiction is **different!**
 - A first step in a legal analysis: what judiciaries have authority in this situation, and which of their laws are applicable?
 - Cross-jurisdictional generalisations are dangerous, as are naïve summaries. (I am not providing legal advice here. ;-)
- Modern states enforce **ownership rights**, making it illegal (or actionable in a civil suit) for non-owners to do certain things to an owned object.
 - An owner can sell property (if it’s “alienable”), or issue a license-to-use e.g. by lease or rental.
 - I’ll survey the “intellectual property” aspect of software, with respect to US law.

U.S. Patents, Trademarks, Copyright

- **Patent:** “the right to exclude others from making, using, offering for sale, or selling the invention in the U.S. or ‘importing’ the invention into the United States.”
- **Trademark:** “a word, name, symbol or device which is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.”
- **Copyright:** “the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of [it], to perform [it] publicly, or to display [it] publicly.”

Source: US Patent and Trademark Office, “What Are Patents, Trademarks, Servicemarks, and Copyrights?”, October 2015, available http://www.uspto.gov/patents/resources/general_info_concerning_patents.jsp#heading-2.

U.S. Patents: Basics

Three types of patents:

1. **Utility** patents: “... new and useful process, machine, article or composition of matter, or any new and useful improvement thereof”
2. **Design** patents: “... new, original, and ornamental design for an article of manufacture...”
3. “**Plant** patents may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant.”

Every country has its own laws...

- “People often talk about software patents
 - what exactly do they mean?
- “The term ‘software’ is considered [by the EPO] to be ambiguous, because it may refer to
 - a program listing written in a programming language to implement an algorithm, but also to
 - binary code loaded in a computer-based apparatus, and it may also encompass
 - the accompanying documentation.
- “... in place of this ambiguous term the concept of a computer-implemented invention has been introduced.”

Source: “Patents and Software? European Law and Practice”, available <http://www.epo.org/news-issues/issues/software.html>, 11 Aug 2013.

NZ Copyright

- Applies to eight categories of “work or type of material”:
 - literary, dramatic, artistic, musical works;
 - sound recordings, films;
 - “communication works” (e.g. TV broadcasts);
 - “typographical arrangements of published editions”.
- Term of copyright protection depends on the type of work:
 - “Artistic works industrially applied” : 16 years
 - “Artistic craftsmanship industrially applied” : 25 years
 - Other categories: 25 to 50 years.
 - Note: US copyright lasts **much** longer than this.
 - “Life of author plus 70 years”; for works of “corporate authorship”, 120 years or 95 years after publication, whichever comes earlier”. (1998 Copyright Term Extension Act)
 - Note: Mickey Mouse was first published in 1928. $1928+95 = 2023$.
 - 2019 is another important year for US copyright.

Source: MBIE, “Copyright Protection in New Zealand”, last updated 24 December 2015. Available: <http://www.mbie.govt.nz/info-services/business/intellectual-property/copyright/copyright-protection-new-zealand/>, 12 September 2015.

Exceptions to NZ Copyright

- There are a few exceptions to NZ copyright:
 - “Fair dealing”: criticism, review, news reporting, research or private study;
 - Limited copying for educational, bibliographic or archival purposes;
 - “Subject to certain conditions, the making of a back-up copy of a computer program”;
 - “time-shifting” of a television programme.
 - In 2008, a new exception was added (Sec 81A): format-shifting for audio recordings, if acquired lawfully and for personal or household use (but not for uploading onto file-sharing systems, or for friends)
- “Fair Use” in the US is a entirely different legal concept
 - NZ copyright covers **all** uses of copyright material, with the specific exceptions noted in the text of the law
 - Anyone accused of infringing US copyright has a broad (and somewhat flexible) defence called “fair use” (17 USC 107):
 - “In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include: the purpose and character of the use...”

“Hard” vs “Soft” Security

- Boaz Barak believes that all important systems should have “well-defined security”.
 - These systems can only be compromised if the analyst’s assumptions (e.g. about the secrecy of cryptographic keys) are invalid.
 - Assumptions can be checked for validity by anyone.
 - Security proofs can be validated by anyone.
 - See http://www.math.ias.edu/~boaz/Papers/obf_informal.html

Boaz's Argument (in brief)

- “Of course, as all programmers know, using rigorously specified components does not guarantee that the overall system will be secure.
- “However, using fuzzily specified components almost guarantees *insecurity*.”

Is it Feasible to Specify Well?

- “The only problem is that it is very very difficult to build such “perfect” systems that are *large*.
- “In spite of this, with time, and with repeated testing and scrutiny, systems can converge to that bug-free state ...
- “Such convergence cannot happen if one is using fuzzily secure components.”

Do you agree with Boaz?

Soft security: Necessary?

- I believe that only a few isolated, stable systems will ever converge on Boaz' ideal bug-free state.
 - Features are added and modified
 - Novel, unexpected uses: are these exploits or appropriate?
 - Systems interact with other systems in complicated, unstable, and unpredictable ways. (“Secure functional composition” is a research area, not a standard practice.)
- Do you trust your bank? Your credit card?
 - Human error is possible (e.g. Westpac Rotorua teller's misplaced decimal point)
 - Fraud is possible
 - Software is buggy, even if it is carefully verified (e.g. Ariane 5)
 - One coping strategy: “trust but verify”

My View of “Soft” Security

- Putting speedbumps on roads doesn’t stop all drivers from speeding, just as “speed bump” security (warning messages, propaganda, lamer-level defences) won’t stop a determined and skilled attacker.
- That doesn’t mean you should ignore “soft” defenses!
- If a secure system is illegal, immoral, unaffordable, or difficult to use, then it will be a target for attack by its legitimate users and its other stakeholders (e.g. the folks who are harmed by its illegal activity).
 - If a system meets Barak’s goal of “well-defined security” but is unaffordable, difficult to use, immoral, or illegal, is it a successful design? I think not...