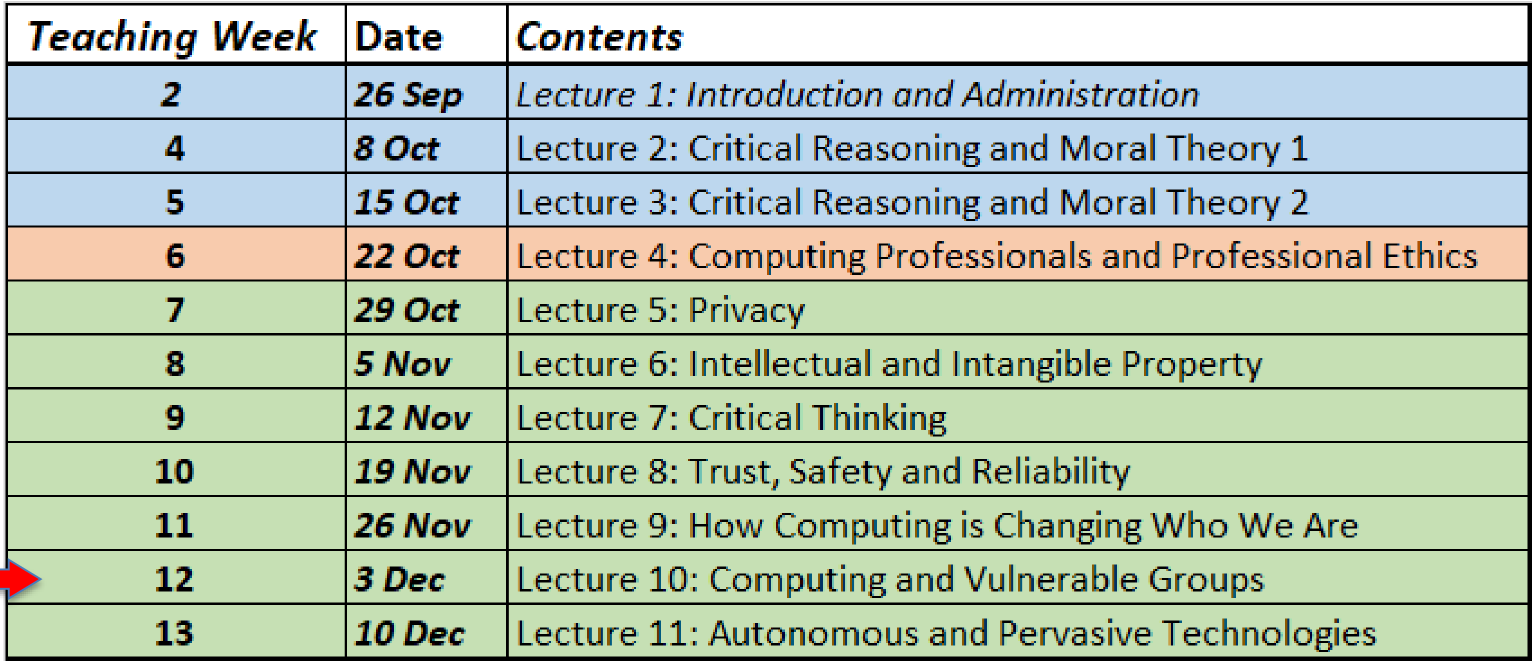
Computing and Vulnerable Groups

Professional Ethics in Computing

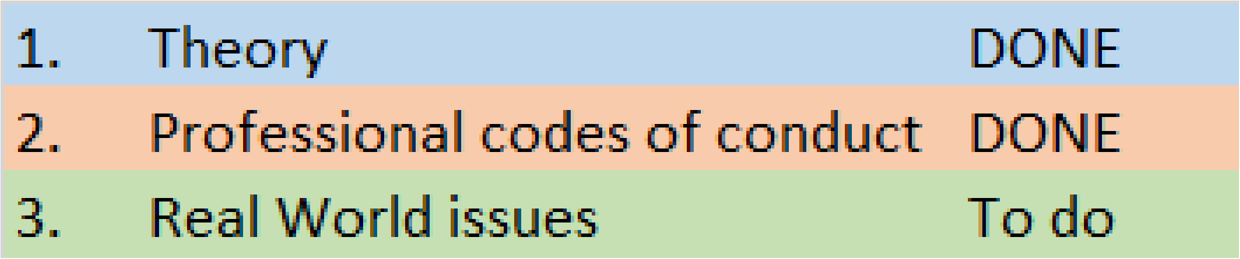
Lecture 10

(Largely based on lecture by J. Cartlidge)

Module Plan & Progress



Teaching Week	Date	*Contents*
2	***26 Sep***	*Lecture 1: Introduction and Administration*
4	***8 Oct***	Lecture 2: Critical Reasoning and Moral Theory 1
5	***15 Oct***	Lecture 3: Critical Reasoning and Moral Theory 2
6	***22 Oct***	Lecture 4: Computing Professionals and Professional Ethics
7	***29 Oct***	Lecture 5: Privacy
8	***5 Nov***	Lecture 6: Intellectual and Intangible Property
9	***12 Nov***	Lecture 7: Critical Thinking
10	***19 Nov***	Lecture 8: Trust, Safety and Reliability
11	***26 Nov***	Lecture 9: How Computing is Changing Who We Are
12	***3 Dec***	Lecture 10: Computing and Vulnerable Groups
13	***10 Dec***	Lecture 11: Autonomous and Pervasive Technologies



1.	Theory	DONE
2.	Professional codes of conduct	DONE
3.	Real World issues	To do

Coursework 2 Deadline: **23:59** on **12/12/2018** (submitted by Moodle)

Notes: Group 10

Qu: Walking along, you bump into somebody. What do you do?

- Say “Sorry” and keep on walking?

Qu: Imagine you bump into a small child. What do you do?

- Check the child is uninjured?
- Find parent/guardian and apologise before walking off?

Distinction between **children** and **adults** is important ethical concern for computing professionals

- ACM/IEEE Software Engineering Code of Ethics and Professional Practice [Rule 1.07] states: “*[c]onsider issues of physical disabilities, allocation of resources, economic disadvantage, and other factors that can diminish access to the benefits of software*”

Today’s aim: To be aware of how the work of computing professionals can **harm vulnerable people in society**

Vulnerable People

We will consider **five** categories of vulnerable people:

1. People **controlled by institutions**
2. People with **limited autonomy**
3. People with **physical limitations of frailties**
4. People with **insufficient resources**
5. People **at risk** of being victims of **hate-motivated behaviour**

…and work through a real-world example (case) of each

NOTE: this is ***not*** an exhaustive list

Vulnerable Groups: *Why Special Attention?*

- From an ethical standpoint, can we justify paying special attention to society's most vulnerable?
- **Qu: What ethical theories may help us?**
  - Rawls' *Theory of Justice*?
    - Use "*veil of ignorance*" argument (even selfish people would choose this type of society, so must be a "*just*" society)
  - Utilitarianism?
    - Take care with "*calculus*" – vulnerable people in minority, but may be disproportionately affected
  - Noddings' *Ethics of Caring*?
    - If we don't have a personal relationship with a person in a vulnerable group, are we obliged to care?

Threat Analysis Method

- **Threat Analysis—**computer security method for systematically identifying ways a technology may be vulnerable to malicious attack
  - Who might want to abuse the system?
  - Why would they want to do so? (i.e., what will they do with the system that they shouldn’t be doing?)
- **Computer security—**design strategies to mitigate risks identified in thread analysis.
  - **Protection:** Address vulnerabilities in the system
  - **Assumption:** threats will always exist, so try to remove vulnerabilities
- **Society—**can use these methods to protect vulnerable groups
  - **Threat analysis**—identify those who might exploit a vulnerable person and explain why
  - **Protection**—implement new laws or policies that attack the threat. Take actions to reduce source of vulnerability.

- Prisoners
- Military Personnel
- Persons living under oppressive governments

1. PEOPLE CONTROLLED BY INSTITUTIONS

Persons subject to institutional control

- People in institutions that take away liberties
  - Prisoners, permanent hospital residents, members of military, citizens under repressive governments, …
  - Most agree it’s ethically justified to remove liberties from certain people (e.g., murderer)
  - Vulnerable to decisions made by those in control
    - Opportunity for intentional/unintentional abuse
- Impact of computing technology:
  - **Positive—**increase personal liberty (new outlets for communication and organisation)
  - **Negative—**whoever controls online activities has greater degree of control over lives

Case: Gun-Camera Videos

- US Military vehicles include gun cameras that shoot footage of whatever the gun is pointed at
  - For commanders to review soldier's actions
  - To evaluate and refine tactics
  - To verify if target killed
  - To identify "friendly fire" incidents
- Wikileaks has posted leaked gun-camera footage
  - US assault helicopter killing two journalists after mistaking camera for a rocket-propelled grenade
  - Then fires on mini-van, two children in the van wounded

https://www.theguardian.com/world/2010/apr/05/wikileaks-us-army-iraq-attack

Case: Gun-Camera Videos

- Opinion of some commentators: **Soldiers' Actions illegal**
  - Attacks are war-crimes and soldiers morally blameworthy
- Opinion of the military: **Soldiers' Actions legal**
  - Attacks lawful and based on reasonable interpretation of facts
- Gun-camera footage is usually classified / not public
  - Why? Soldiers required by profession to do things not ordinarily considered moral

Qu: Do gun cameras make soldiers vulnerable to harm?

Qu: Should US military release gun camera footage publicly, online?

Qu: Should US military stop using gun cameras altogether?

- Mentally disabled persons
- Children, particularly orphans

2. PEOPLE WITH LIMITED AUTONOMY

People with limited legal autonomy

- Entity has "***autonomy***" if it is free to make decisions without outside constraints/interference
  - (more next week)
- Children have little legal autonomy
  - (parents/guardian)
- People with mental illnesses or disabilities
  - (if ruled legally incompetent)
- The elderly
  - (with onset of dementia)

People with Limited Autonomy

- Vulnerable because they depend on the good will and attention of guardians
- Such people disproportionately targeted by wrongdoers as less likely to protect themselves
- When computer systems fail; people with limited autonomy have higher likelihood of being harmed as they cannot easily correct errors/seek redress

Case: Cell-Phones and Family Locator Services

- Family locator services allow the owner of a mobile phone to keep track of location (also keeping track of phones user)

  1. Phones located by GPS, cell-phone signal an Wi-Fi. Turning of GPS does not stop locator from working
  2. Family locator works only for cell phones that are all on a simple family cell phone plan
  3. A **locator** is anyone who has permission to see location of others. Owner of plan is a locator, but can also designate others
  4. A **locatee** is anyone whose cell phone is being tracked. Account owner decides which family members
  5. A person can be a locator and locatee (e.g., owner/spouse)
  6. Can be set to send SMS messages based on time and location conditions (e.g., child leaves school during school hours, SMS sent to parents)
  7. Can restrict cell phone service based on location/time of day. E.g., cannot send SMS on school grounds during school hours.

How should the locator system be used?

Qu: List possible “chilling effects” this system could have. What kind of things might teenage children chose not to do? (even though they are technically allowed)

Qu: If all family members are locators and locatees; what are some possible chilling effects on adult family members?

Qu: What are harms of being a locatee? Are children more vulnerable to these harms?

Qu: Assume the premise that all adults (parents, grandparents, etc.) should be locators, and young children locatees. At what age should a child no longer be a locatee? What about a university student still on parents’ cell phone plan?

Qu: Should phones of locatees display icon so users know they are being tracked?

Qu: Should it be possible for locatees to turn off the location feature?

- The elderly
- Physically disabled persons
- Pregnant women
- Dying patients

3. PEOPLE WITH PHYSICAL LIMITATIONS AND FRAILTIES

People with physical disabilities

- Face challenges using new technology (because tech **not accessible**)
- Tech that promote accessibility:
  - **Screen-readers** (read text audibly; vision impairments)
  - **Predictive typing** (people with motor control problems)
  - **Subtitles** (display text of audio; hearing impaired users)
  - **High contrast displays** (text easier to read; vision impair)
  - **Haptic feedback** (cell phone vibrate; hearing/vision impair)
- Tend to be more dependent on tech than other people

Case: Hackers & Implantable Medical Devices

- Imagine if a computer hacker sitting near you could (at the press of a button) stop your heart!
  - For >3million people with "implantable cardiac defibrillators" (ICD), this is a true concern!
  - ICD: Auto-detect rapid/irregular heartbeat (V-Fib)
    - administer electric shock to restore normal rhythm
    - report back to health care practitioner
  - ICD reports can be read, and ICD re-programmed via radio signal
  - ICD can also ***cause*** V-Fib!
    - used by doctors on implant, to check it works correctly
  - Therefore, possible to cause heart-attack remotely

Case: Hackers & Implantable Medical Devices

- *Halperin et al.* found defective security features:
  1. ICD only broadcasts info when a powerful magnet is nearby. However, ICD still accepts commands so does not prevent V-Fib.
  2. Radio signals have limited range, so must be close to patient – but attacker can modify programming console to boost signal
  3. ICD manufacturers keep communication protocols secret ("security through obscurity"). But if hacker has access to genuine programming console, this provides no protection
- It is possible to trigger V-Fib without programming console by recording and replaying the message that initiates intentional V-Fib
- Anyone who has access to console can cause great harm (and more than 500,000 implanted every year!) so hard to keep under control.

Possible Solutions to ICD Hacking

- Denning et al. proposed solutions to ICD hacking
- **Qu: Rank the possible security proposals, below.** Consider human values as well as technical issues
  a) Do nothing and continue to use current system
  b) Remove the feature that makes it possible to intentionally cause V-Fib (a hacker could still possibly turn off the ICD)
  c) Require patient to memorize PIN to gain access
  d) Tattoo PIN on patient that must be entered
  e) Patient to permanently wear bracelet that sends out radio signal. If signal present, ICD ignores programming console

- The poor
- Workers with obsolete skills or those who are not permitted to organize in unions

4. PEOPLE WITH INSUFFICIENT RESOURCES

The Poor

- Often lack access to computing/communications
  - Some have little food/water, *much less Internet access*!
- Access to high-quality education limited
  - Reducing person's ability to benefit from tech
- Legal help too costly be a real option
- Receive less benefit from computing tech than upper/middle classes
  - **digital divide**—the gap between tech haves/have-nots

Case: PTA Newsletters

- PTA—A community group made up of parents and teachers of a school group
  - PTA mission—to improve school experience
  - Elementary school—ages 4-11; 700 students in total
  - Each month, PTA president posts all parents a physical newsletter (whether or not they attend PTA)
  - **Problem:** $1 each printed newsletter, total cost $6,300/school year
  - **Solution:** Send by e-mail. $0 cost
    - **But school could only get hold of 90% of parents' emails**
  - **Digital divide**: between children with parents' emails collected and those without emails collected
    - families who had regular e-mail access vs. families headed by night-shift workers, people who don't own cars, the homeless, people in a shelter for domestic violence

PTA Newsletters: Other options available

- Mail physical copies to the 70 families left out? (i.e., without email)
  - cost $1800/year
  - No discounts available for large volume printing/posting
- Print 70 copies, hand these out to children at school
  - cost $900/year
  - No posting costs
  - **Qu: Can you see any potential problems with this option?**
  - Teachers objected that it singles out vulnerable children in the classroom.
  - Fear: children would be labelled “poor kids”. These children already vulnerable, so teachers did not want to single them out

Qu: Is there a better alternative option?

- Racial or ethnic minorities
- Religious minorities
- Minorities of gender identity or sexual preference

5. PEOPLE AT RISK OF BEING VICTIMS OF HATE-MOTIVATED BEHAVIOUR

Minority Groups

- Discrimination against minority groups can make more difficult to benefit from tech and seek legal redress for harms caused by tech
- International (and anonymous) targeting by hate groups
- Here we consider racial minorities and gender identities

Case: Assumptions behind demographic questions

- *"I just realised that race is something I have to think about", [a student applying for college] wrote, describing herself as having Asian mother and a black father. "It pains me to say this, but putting down black might help my admissions chances and putting down Asian might hurt it."*
  - *New York Times (2011)*

Qu: What is happening here?

Q1. What is your race?

○ White, not of Spanish or Hispanic origin

○ Spanish or Hispanic origin

○ Black

○ American Indian or Alaskan Native

○ Asian

○ Pacific Islander

- Radio buttons often chosen to enable a simpler data model
- Makes sense from a data-base administration perspective
- But has real-world ethical consequences

Traditional radio buttons forces a multiracial person to make an inaccurate statement

Q1. Are you of Spanish or Hispanic origin?

○ Yes ● No

Q2. What is your race? Tick all boxes that apply.

□ White

☑ Black

□ American Indian or Alaskan Native

☑ Asian

□ Pacific Islander

Checkbox design allows greater accuracy

Sex / Gender Choices

- Traditionally sex/gender was a binary choice:
  - male/female
- Google+ then moved to three choices:
  - male/female/other
- Facebook now offers 71 choices in UK
- Google+ now has freeform textbox (infinite choice)

Qu: Which approach to sex/gender on social networks is morally preferable? (use ethical reasoning)

http://www.theverge.com/2014/12/11/7375871/google-introduces-gender-options-for-its-social-network

http://www.telegraph.co.uk/technology/facebook/10930654/Facebooks-71-gender-options-come-to-UK-users.html

Summary

- ***ACM/IEEE Software Engineering Code of Ethics*** explicitly requires software engineers to consider vulnerable groups
- ***The difference principle*** (Rawls) provides some ethical support for the idea that vulnerable groups are special
- **Utilitarianism**—vulnerable groups may need special consideration because they tend to be easily overlooked or forgotten (leading to incorrect calculations)
- **Threat analysis** can be used to analyse society, and mitigate threats to vulnerable groups

Related Reading

- Brinkman & Sanders, *Ethics in a Computing Culture* (2013), Chapter 8.
- Denning et al. (2010), *“Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices*”. Proc. 28th Int. Conf. Human Factors in Computing Systems (CHI-2010). Atlanta, GA, April: ACM, pp. 917—926.
- Cheryl Gerber, *"Ex-La. gov, 83, marries 32-year-old prison pen pal"*, USA TODAY, 29 July, 2011.
- S. Saulny and J. Steinberg, *"On College Forms, a Question of Race, or Races, Can Perplex"*, The New York Times, 13 June, 2011.
- J. A. Vargas, *"For Gay Gamers, A Virtual Reality Check"*, Washington Post, 11 March, 2006.
- World Health Organisation (WHO), *"What do we mean by 'sex' and 'gender'?”*