Intro

CITS3200 Ethics Case Studies.
This is a set of simple Case Studies designed to help you understand some of the Ethical Issues you may face as a computer professional.
Your responses will be recorded and aggregated with others from the 2020 CITS3200 Class (they will be kept anonymous).
Average responses will be published in a table later this Semester (with comparisons from earlier years).
You may suspend answering at any time and resume later (provided it's from the same device, and within a week). After 10 cases, you may exit the "survey", or go on with another 7.

Please click the Next button when you are ready to proceed.

How to Analyse Cases

How to go about analysing these Cases:
Note that these studies are mostly based on actual cases, and are aimed at elucidating ethical or social issues that you may be faced with. The ACS Code of Ethics provides some basis for making good choices.
You might find it useful to use the "Social Contract" approach (see www.iep.utm.edu/soc-cont/), which involves the following steps:

- identify those in the scenario to whom you owe any kind of duty;
- assess the extent of harm potentially incurred by each person or category of people;
- assign priorities to the duties owed;
- identify possible alternative courses of action;
- seek opportunities for negotiation and formation of "social contracts" with the various stakeholders.

Note that the are often no "correct answers" - decisions are based on value judgements, and there will be differences of opinion at times...

Please click the Next button when you are ready to start.

Q1b

Case Study 1b: Developing Software for On-Line Ordering/Payment
Suppose you are the manager of a small software development team, charged with developing an on-line ordering and payment system for your Company. You estimate that it will take 6 months, for you and your 2 programmers.
You tell the client department that it will be ready in 6 months.
After 3 months has elapsed, you find that instead of 6 months is it going to take 12 months (ie an extra 6 months), for the following reasons:

- the user specification changed, costing 1.5 months;
- regulatory requirements changed, costing another 1.5 months;
- you encountered some unforeseen technical difficulties, costing 1 month;
- one of your programmers resigned, costing 1 month;
- you were actually too optimistic in the first place, adding 1 month.

What do you do (what is at stake? to whom do you have a responsibility?):

1. Resign: it's all too hard, go and work in a fast food shop

2. Work unpaid double-time, you and your team, enabling you to finish on time

3. Tell Management that it will not be ready on time, and nothing can be done about it (blame it all on the changes foisted upon you)

4. Adopt a combination of 2 and 3, ie work some extra time, but don't take the blame

5. Offer to introduce a cut-down version after 7 months (only 1 month late), but with no credit card checking and manual delivery of credit card debits to the clearing house

Do something else: What?

Q2

Case Study 2. Downloading on Company Internet
Suppose you are the Systems Administrator for your medium-sized Company.
Your Company has a Policy that allows “moderate” use of Company computers and Internet access for private purposes.
In the course of monitoring traffic levels, you notice very high incoming traffic volume to one computer within the Company.
Upon investigation, you believe that one employee is downloading large quantities of MP3 files.

What action do you take?

1. Impose a "throttle" on the line to that PC

2. Take up the matter with the employee in question

3. Report the matter to your/their boss

□ Take some other action: What?

Q3

Case Study 3: SDMI Challenge
Worried about pirating of music files, on 6-Sep-2000 the Music Industry launched the Secure Digital Music Initiative. The aim was to develop a secure encryption for all music files, which then could only be played on SDMI-compliant players. It would not be possible to copy and distribute files (other than for backup). They developed an "unbreakable" watermarking system (steganography). They issued a public challenge, offering $10,000 to anyone who could break their encryption. This was boycotted by some groups, while a group at Princeton University was able to break the code, but refused the reward.

Which of the following do you think is the right approach?

1. Boycott the Challenge (you think it's a dastardly idea)
2. Break the code, publish your solution, collect the reward (go public, but take the loot - why not?)
3. Break the code, publish your solution, but do not collect the reward (a rather altruistic approach)
4. Break the code, don't publish your solution, collect the reward (what SDMI might have been looking for)
5. Break the code, don't publish your solution, don't collect the reward (might give you an edge if they ever put this into production)

Q8

Case Study 8: Examining Someone's Email
Suppose you are the Systems Administrator at your medium-sized Company. Your Company does not allow its systems to be used for private email, ie only for Company business. Your boss requests you to obtain all the email over the past week to and from a particular employee.

What do you do?

1. Just comply (he is the boss, after all)
2. Comply, but you tell the employee in question (you think they have a right to know)
3. Refuse the request unless the employee has given their consent (you think their privacy should be protected)
4. Escalate the matter to higher management for a ruling
5. Just refuse (you can't think of a legitimate reason why the boss should want this)

How Important Here is the Clarity of Company Policy?
For instance, might you change your mind if the Company had no clear policy on private use of email?

Yes, I would have a different response

No, it would make no difference to my response

I'm unsure...

How Important Here is the Clarity of Company Policy?
For instance, might you change your mind if the Company made it clear that it reserved the right at any time to examine any Company email?

Yes, I would have a different response

No, it would make no difference to my response

I'm unsure...

Q9

Case Study 9: Examining Private Email.
Suppose you are the Systems Administrator at a university college.
The university and the college have strict rules about respecting the confidentiality of private email.
One of the college students, an under-age 14 year-old girl, has gone missing.
The college Warden asks you to provide copies of all email to and from this student during the past month, so they can be examined for clues as to her associates and whereabouts.
What do you do?

1. Just agree (it's important to find her, and isn't the Warden "in loco parentis"?)

2. Agree to do so, but only with the consent of the student's parents (they ought to be the ones to ask)

3. Agree to do so, but only if an official request is made by the police (ie an official "missing person" enquiry)

Take some other action - What?

Would it make any difference if only the parent(s) had asked, and no-one else (ie not yet an official missing person enquiry)?

Yes, they are the only ones with the authority to ask

No, the Warden is after all "in loco parentis"

I'm not sure...

Q10

Case Study 10: Accidental Partial Disclosure of Email
Suppose you are the Systems Administrator at a medium-sized Company. The Company has strict rules about email confidentiality (and does allow a certain amount of private email).
In the course of routine system checking, you come across fragments of email that appear to indicate that a male workmate is having an affaire with the wife of your friend (who works somewhere else).
Your friend is suspicious and asks if you have seen any evidence to support this suspicion.

What do you do?

1. Pretend that you know nothing, and do nothing more

2. Say nothing to your friend, but henceforth monitor all email to/from that workmate, looking for conclusive evidence

3. Say nothing to your friend, but confront that workmate (in the interests of helping your friend)

4. Say nothing to your friend, but keep alert for any evidence from some other source to corroborate this suspicion, and only then share with your friend

Take some other action: What?

Would it make any difference if, instead of indicating an affaire, the email fragment had indicated one of the following?

The email indicated that the workmate was ripping off the Company

The email indicated that the workmate was compromising another worker

The email indicated that some illegal activity was being planned

Q11

Case Study 11: Responsibility for Virus Protection
Suppose that you are the System Administrator for a medium-sized company.
Your company does allow use of its systems for private email, and has a strong confidentiality policy covering that email.
However, the volume of email-borne viruses has been on the increase, and staff are not implementing the recommended procedures (eg keeping virus protection up to date). This is creating a lot of additional work for you, to cleanse staff members' computers when they become infected.
You are convinced that a straightforward, and ultimately much less expensive, solution would be to impose a check on all email on entry to and exit from the Company.
However, staff (and the Company managers) object on the grounds that this would make covert email snooping easier.

So, what do you do?

1. Comply with the opposition and leave things as they are
2. Take up the matter with the Company CEO
3. Resign and move to a more "enlightened" employer

□ Take some other action: What?

Q13

Case Study 13: Supervisory Powers
Suppose that you are the Systems Administrator for your medium-sized Company.
You have installed a system that allows a "Common Desktop Environment" or "Standard Operating Environment, SOE" to be deployed throughout the Company, which also provides various tools for remotely monitoring desktop activity - this allows you, for instance, to undertake remote desktop help activity.
Your Boss requests you to install this "supervisory" capability also on their computer. With this, they could monitor all sorts of employee activity, including "snooping".

What do you do?

1. Agree to this request, because the Boss is in charge
2. Agree, but only if employees are all notified that this is being done
3. Agree, but notify the employees yourself that this is being done
4. Refuse, and notify the employees of what the Boss wanted to do

□ Take some other action: What?

Q14

Case Study 14: Security Competence
Suppose you are the Systems Administrator at a medium-sized Company.
Your Company is subject to an increasing (but not yet disastrously high) level of hacker attacks.
Your Company IT Committee agrees that a Firewall should be installed ASAP, and it falls to you as the most competent IT person to do this - and you see this as a great career opportunity.
But you have no experience or knowledge at all of Firewalls.

What do you do?

1. Ask for time and funds to attend a suitable training course - but none is available for some months
2. Scan the Web for suitable self-help information, to enable you at least to learn the basics and use the correct jargon
3. Quickly buy and devour a suitable text, such as Firewalls for Dummies
4. Recommend employing a firm of technical consultants to advise the details of the way forward

□ Take some other action: What?

Q15

Case Study 15: Systems Security Responsibility
Suppose you are responsible for Computer System Security at your medium-sized Company.
You have formulated and received Company approval for a backup policy, which requires all computer users to undertake backups at least once per week.
However, you are still continually asked to retrieve lost files, which have not been properly backed up; this is costing you a lot of time which you can't afford, and nor have you the time to constantly badger staff to undertake these backups.

So what do you do?

1. Just put up with it, trying to balance calls upon your time as best you can
2. Continue nagging staff to do the backups, but really with little hope that things will improve
3. Complain officially to Management, perhaps fingering some individual(s)
4. Request approval to spend large amounts of money on automating central backups
5. Resign and join a Company that does take this matter seriously

□ Take some other action: What?

Review

Helpfulness of these Case Studies

Did you find these Case Studies Helpful?

Yes, and I had not previously thought much about Ethics in ICT

Yes, and I did already have some understanding of Ethics in ICT

Neutral, their usefulness was marginal

No, I already had a good understanding and they didn't add much

No, I didn't find them helpful or relevant

Do you have general comments to make about the nature and/or usefulness of these Case Studies as a means of stimulating interest in Ethics in ICT?

Enter your thoughts here:

Other Ethics Case Studies
There are many examples of more interesting, challenging and complex Case Studies available at various places on the Web, in particular ones that explicitly relate to the ACS Code of Ethics. See for example https://www.acs.org.au/governance/ethics-committee.html (scroll down).

A selection of thought-provoking case studies was published in the ACS publication Information Age in Oct/Nov 2018 - see https://ia.acs.org.au/article/2018/ethics-part-1--artificial-influencers.html (scroll down to see several more)

There are also some helpful Case Studies in the following publications:

- Burmeister, Oliver K: “Applying the ACS Code of Ethics”, Information Age, Feb/Mar 2001, pp54-59, and in the subsequent 3 issues (Apr/May, Jun/Jul, Aug/Sep, 2001). Also published as: Burmeister, Oliver K: “Applying the ACS Code of Ethics”, Ethics in Computing, v32, n2, May 2000, pp107-119.
- Anderson, Ronald E et al: “Using the New ACM Code of Ethics in Decision Making”, Communications of the ACM, v36, n2, Feb 1993, pp98-106.
- Bynum, Terrel Ward & Rogerson, Simon, eds: “Computer Ethics & Professional Responsibility: Introductory Text & Readings”, Blackwell, 2004.
- ACM Code of Ethics Case Studies - see https://www.acm.org/code-of-ethics/case-studies .

There are several more simple case studies to follow in the rest of this "Survey", which you are encouraged to also look at and respond to.

Do you wish to proceed with these extra case studies (or exit now)?

Yes

No, exit now

Q16

Case Study 16: Unintelligible Reports to Management

Suppose that you are responsible for Computer Systems Security at your medium-sized Company.

You identify some areas of vulnerability, and prepare a Report to Management setting out the measures that need to be put in place to address these vulnerabilities; the Report is largely written in terms of which "network ports" should be blocked in a Firewall.

Management cannot understand your Report and will not act until they better understand what steps you are advocating. You cannot think how else to express what you recommend. There is no-one else in the Company that might be able to help.

So, What do you do?

1. Refuse to rewrite it - they should just trust you, and if they don't it's their fault
2. Take a course in "clear English expression" to enable you to rewrite the Report in clearer terms
3. Contact a colleague at another Company (or perhaps at the Computer Society) to ask for help
4. Ask for funds to engage a technical writer to rewrite the Report
5. Ask for funds to engage an external consultant to prepare an alternative Report

□ Take some other action: What?

Q17

Case Study 17: Blaming the Computer

Suppose that you are the IT Manager at a small government department.

A recent computer problem resulted in many regular cheques to pensioners being delayed by several weeks.

The Minister responsible has prepared a Press Release in which the problem is blamed on a "Computer Malfunction".

However, you know the the problem was caused (only) by the following factors:

- rapid changes made to an operational system in order to accommodate changes required by the Minister;
- a poor system specification for the changes;
- a consequent programming error.

So, what do you do?

1. Keep quiet; what the Minister says is their business
2. Complain to the Minister's Office that this is misleading
3. Take up the matter with your Head of Department, as it unfairly blames the computer

□ Take some other action: What?

Q18

Case Study 18: Quick Patch versus Full Rewrite

Suppose you are the IT Manager at a small government department.

You have been requested by the relevant Government Minister to make some changes to a key operational computer system, and to make them within 2 weeks.

It had already been agreed that this system is at "end of life" and cannot safely be patched any further, but must be completely rewritten; this will take at least 6 months, and work has already commenced.

Any quick patches carry a very high risk of the whole operational system failing.

What do you do?

1. Refuse the Minister's request - it is just not safe to do so (but with all the political fallout, and consequences for your career, that may entail)

2. Endeavour to comply as best you can, without making a fuss about it

3. Comply with the request, but make quite sure that you have on record that you strongly oppose this action

Take some other action. What?

Q19

Case Study 19: Project Estimation Errors

Suppose you are the IT Manager for a medium-sized Company.

Your team has been embarked for the past 4 months on the development of a major system of critical importance to the Company.

You discover that progress to date has been only been about a half of what you had planned, mainly because your estimates had been greatly optimistic, in order that your team be awarded the contract for this work.

Many other parts of the Company are dependent on delivery of this system on-time.

What do you do?

1. Keep quiet and hope the problem "goes away"

2. Encourage your team to redouble their efforts to catch up for lost time

3. Take on more staff to speed up development

4. Blame the delays on "external factors", like programmer illness, specification creep, etc

5. Frankly confess your wrong estimates to Management, thus risking losing credibility and any further work (and possible redundancies in your team)

Take some other action: What?

Q21

Case Study 21: Investigate Suspicious Activity
Suppose you are the Systems Administrator at a medium-sized Company.
Someone reports to you (anonymously) that PersonX has been using company computer systems and Internet access to download hard-core pornographic material.
If you go to PersonX and confront them (or raise the matter with them in a more delicate fashion), you recognise that they will almost certainly deny it, and they will quickly remove all the evidence.

What do you do?

1. Ignore the allegation

2. Using your system privileges, first check out the report you've received, and only if confirmed do you confront PersonX

3. Using your system privileges, first check out the report you've received, and if confirmed take the matter to your or PersonX's boss

4. Report the matter immediately to PersonX's boss, not giving PersonX the opportunity to delete the material

Take some other action: What?

Would it make any difference if instead of hard-core pornographic material it had been:

soft-core pornography

child pornography

Q22

Case Study 22: Moderating Employee Discussion Forum
Suppose you are the Systems Administrator at a medium-sized Company.
Your Company has set up an on-line Discussion Forum to encourage employee discussion/participation.
Various employees repeatedly post comments that are very critical of Company policies, practices, etc.
Your boss asks you to change it to become a moderated Forum, with the boss as Moderator, enabling them to refuse any postings they don't like.
You feel this is designed to stifle criticism.

What do you do?

1. Just agree, they are the boss, after all, and the Forum was their idea

2. Argue the toss with the boss, pointing out it could stifle helpful criticism, but then agree

3. Take the matter to senior management, as you think the boss is abusing their position

4. Take the matter yourself to the Forum to ensure the boss' plan gets wide publicity within the Company

5. Go to the local Press with the story

Take some other action: What?

Q23

Case Study 23: Identifying Author(s) of Anonymous Messages

Suppose you are the System Administrator at a medium-sized Company.
Your Company has set up an on-line Discussion Forum to encourage employee discussion/participation, which allows anonymous posts.
The Forum frequently receives anonymous posts which are highly critical of Company pol,ices, practices, etc.
Your boss asks you to identify the author(s) of these anonymous posts (which you are able to do, using your system privileges).

What do you do?

1. Just agree, they are the boss, after all.
2. Argue with the boss that this could stifle useful feedback, but then agree
3. Take the matter to senior management, as you think the boss is abusing their position
4. Use the Forum yourself to ensure this request first gets lots of publicity within the Company
5. Go to the local Press with the story

□ Take some other action: What?

Powered by Qualtrics