
Dependable Systems

dcms.cs.uni-saarland.de/ethics_21/
Sarah Sterz, Kevin Baum, Prof. Holger Hermanns

Training Exercises C4 (Privacy)

with Example Solutions

Issue 1: *Pro Tanto Bad*

In the video we claimed that privacy violations are pro tanto bad. Think about this claim. Give a compelling argument why this is true. Does the same hold for privacy threats?

Sketch of a Solution 1:

Argument:

P1:	If someone's privacy is violated, there is a significant chance that information about them is distributed in a way that is dis-preferred by the person.
P2:	If P1, then privacy violations are pro tanto bad for the person who's privacy is violated.
C1:	Therefore: Privacy violations are pro tanto bad for the person who's privacy is violated. (C1, C2)
P3:	If something is pro tanto bad for someone, it is pro tanto bad.
C:	Therefore: Privacy violations are pro tanto bad. (C1, P3)

One could make a similar argument for privacy threats. However, privacy threats are arguably less (pro tanto) bad than privacy violations, because for mere privacy threats, the chance of an unfavourable distribution of personal information is usually smaller than with privacy violations, because the actual violation has not happened yet.

Issue 2: *Nothing To Hide*

Sometimes, people say things like "I've got nothing to hide, thus surveillance is not bad." Why are they wrong?

Sketch of a Solution 2:

Surveillance can be bad for you even though you do not have anything to hide. The feeling of being watched is proven to cause people to act differently than they otherwise would have had. Also, the mere possibility to do important things unobserved can be seen as valuable, as you can never know

that you will not have anything to hide in the future, either because you really do something bad or because things you now consider normal are seen as something illegal in the future.

As Edward Snowden famously said: "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Issue 3: *Argument*

Come up with a sound argument for or against the following claim or a reasonable conditionalization thereof:

> When it is possible that public security is severely threatened, states are morally permitted to use all or most privacy threatening and violating technologies they have to in order to decrease the possibility of the security threat.

Give sufficient reason to believe in the soundness of your argument.

Sketch of a Solution 3:

Argument:

P1:	*If* it holds that when it is possible that public security is severely threatened, states are morally permitted to use all or most privacy threatening and violating technologies they have to in order to decrease the possibility of the security threat, *then* a very small probability of a threat suffices such that it is morally permissible for states to use all or most privacy threatening and violating technologies they have to in order to decrease the possibility of the security threat.
P2:	There is always a very small probability for all kinds of security threats.
P3:	*If* a very small probability of a threat suffices such that it is morally permissible for states to use all or most privacy threatening and violating technologies they have to in order to decrease the possibility of the security threat *and* there is always a very small probability for all kinds of security threats, *then* it is always morally permissible for states to use all or most privacy threatening and violating technologies they have.
P4:	It is not always morally permissible for states to use all or most privacy threatening and violating technologies they have.
C:	It does not hold that when it is possible that public security is severely threatened, states are morally permitted to use all or most privacy threatening and violating technologies they have to in order to decrease the possibility of the security threat.

Argument: Logical Form

P1:	$a \to b$
P2:	c
P3:	$b \wedge c \to d$
P4:	$\neg d$
C:	$\neg a$

Issue 4: ***Puzzling Arguments***

Professor Clumsy wanted to present his students with some arguments, but messed everything up and forgot which sentences belong to which argument and whether it was a premise or a conclusion. Help Professor Clumsy to sort out everything.

(a) Try to reconstruct as many valid (non-trivial[1]) logical forms as possible from (I).

(b) Try to reconstruct as many valid (non-trivial) tabular forms from (II) as possible.

(c) Can you match your reconstruction from (b) with some of the reconstructions from (a)?

(d) Take a look at your results from (b). Are they sound? If no, attack the arguments.

(e) Take a look at (III). Try to construct two valid tabular arguments and their corresponding logical forms. It holds that every premise and the conclusion of these arguments is at least available in logical or in natural language form in (III).

(f) Take a look at your results from (d). Are they sound? If no, attack the arguments.

(I) a, $\neg a$, b, c, $\neg c$, d, $a \to b$, $b \to c$, $a \vee d$

(II)
- If states ought to promote public safety, they sometimes have to use privacy threatening technologies.
- Citizens cannot reasonably oppose the use of privacy threatening technologies by states.
- States do not have an obligation to promote public safety.
- Citizens can reasonably oppose the use of privacy threatening technologies by states.
- States sometimes have to use privacy threatening technologies.
- States ought to promote public safety.
- If citizens ought not to oppose privacy threats, states sometimes ought to violate their citizens' privacy.
- States sometimes ought to violate their citizens' privacy.
- If states sometimes have to use privacy threatening technologies, then citizens cannot reasonably oppose the use of privacy threatening technologies by states.
- Using CCTV and saving the video is a privacy violation.

(III)
- $P(A)$

[1]For the scope of this exercise (and only this exercise), the following things count as trivial: petitio principii (i.e. the conclusion is one of the premises), arguments from ex falso quodlibet (i.e. premises contradict each other), and nothing else.

- $Q(A)$
- $\forall x.R(x) \rightarrow \neg S(x)$
- All privacy threatening technologies can be privacy violating technologies.
- If CCTV is widely used in public and semi-public areas, it is prima facie bad to use it.
- CCTV can be a privacy violating technoglogy.
- If people have no choice to evade it, the use of privacy threatening technologies is prima facie bad.
- CCTV is a privacy threatening technoglogy.

Sketch of a Solution 4:

(a) (1)

Argument:

P1:	a
P2:	$a \rightarrow b$
C:	b

(2)

Argument:

P1:	b
P2:	$b \rightarrow c$
C:	c

(3)

Argument:

P1:	a
P2:	$a \rightarrow b$
P3:	$b \rightarrow c$
C:	c

(4)

Argument:

P1:	a
P2:	$a \rightarrow b$
P3:	$b \rightarrow c$
P4:	$\neg c$
C:	$\neg a$

(5)

Argument:

P1:	$a \vee d$
P2:	$\neg a$
C:	d

(b) (i)

Argument:

P1:	States ought to promote public safety.
P2:	If states ought to promote public safety, they sometimes have to use privacy threatening technologies.
C:	States sometimes have to use privacy threatening technologies.

(ii)

Argument:

P1:	States ought to promote public safety.
P2:	If states ought to promote public safety, they sometimes have to use privacy threatening technologies.
P3:	If states sometimes have to use privacy threatening technologies, then citizens cannot reasonably oppose the use of privacy threatening technologies by states.
C:	Citizens cannot reasonably oppose the use of privacy threatening technologies by states.

(iii)

Argument:

P1:	States ought to promote public safety.
P2:	If states ought to promote public safety, they sometimes have to use privacy threatening technologies.
P3:	If states sometimes have to use privacy threatening technologies, then citizens cannot reasonably oppose the use of privacy threatening technologies by states.
P4:	Citizens can reasonably oppose the use of privacy threatening technologies by states.
C:	States do not have an obligation to promote public safety.

(iv)

Argument:

P1:	States sometimes have to use privacy threatening technologies.
P2:	If states sometimes have to use privacy threatening technologies, then citizens cannot reasonably oppose the use of privacy threatening technologies by states.
C:	Citizens cannot reasonably oppose the use of privacy threatening technologies by states.

(c) Matching: (1) and (i), (2) and (iv), (3) and (ii), (4) and (iii)

(d) (i) seems to be sound, (ii) – (iv) are not: "If states sometimes have to use privacy threatening technologies, then citizens cannot reasonably oppose the use of privacy threatening technologies by states." is not true, as citizens can reasonably oppose the use of those technologies, if the extent of that use is too large.

(e)

Argument: Tabular Form 1

P1: All privacy threatening technologies can be privacy violating technologies.
P2: CCTV is a privacy threatening technoglogy.

C: CCTV can be a privacy violating technoglogy.

Argument: Logical Form 1

P1: $\forall x.P(x) \rightarrow Q(x)$
P2: $P(A)$

C: $Q(A)$

Argument: Tabular Form 2

P1: If people have no choice to evade it, the use of privacy threatening technologies is prima facie bad.
P2: If something is widely used in public and semi-public areas, people have no choice to evade it.
P3: CCTV is a privacy threatening technoglogy.

C: If CCTV is widely used in public and semi-public areas, it is prima facie bad to use it.

Argument: Logic Form 2

P1: $\forall x.\neg S(x) \rightarrow (P(x) \rightarrow T(x)$
P2: $\forall x.R(x) \rightarrow \neg S(x)$
P3: $P(A)$

C: $R(A) \rightarrow T(A)$

Issue 5: *Contextual Integrity*

Apply Helen Nissenbaum's contextual integrity approach to the following situations. It may be necessary to do a case analysis.

(a) A friend of yours tells you a secret, namely that she is homosexual but not yet ready to have her coming out. You promise not to tell anybody else. You break that promise by telling your little brother.

(b) A fitness tracker collects GPS data and, unbeknownst to the user, sends it to the manufacturer who sells it for money.

(c) Your tutor talks about how you performed in your last assignment with the lecturer.

(d) Your tutor talks about how you perform in your assignments with his flat mate.

(e) A secret service intercepts and collects all of your communication, because they rightfully believe that you are a terrorist.

(f) A secret service intercepts and collects all of your communication, because they intercept and collect everybody's communication.

Sketch of a Solution 5:

The context and/or transmission principles might vary in your solution, since once more there is not only one correct answer.

(a) **context:** friendship
actors: you (sender), your little brother (information recipient), your friend (information subject)
attributes: name, sexual orientation
transmission principles: sender confidentiality, consent
Both negative norms are violated, since you were supposed to keep the secret confidential and your friend did not consent to you telling this to your brother.
The contextual integrity is **violated**.

(b) **context:** business
actors: fitness tracker (sender), manufacturer (information recipient), users of fitness trackers (information subject)
attributes: GPS data
transmission principles: notice, consent, need, entitlement
Which transmission principles are adequate here is debatable. However, at least notice, probably even consent are transmission principles, and in the given example, the user is not even notified, thereby at least one negative norm is violated, so:
The contextual integrity is **violated**.

(c) **context:** education
actors: your tutor (sender), your lecturer (information recipient), you (information subject)
attributes: name, performance in last assignment
transmission principles: entitlement, most plausibly also need
The lecturer is entitled to know the performance of his students and therefore the tutor has to provide the information. Also, the lecturer probably needs to know your performance.
The contextual integrity is **preserved**.

(d) **context:** education, friendship
actors: your tutor (sender), his flatmate (information recipient), you (information subject)
attributes: name, performance in assignments
transmission principles: sender confidentiality
The negative norm is violated.
The contextual integrity is **violated**.

(e) **context:** Crime investigation
actors: the secret service (sender), the secret service (information recipient), you (information subject)
attributes: all your communication
transmission principles: need? entitlement?
In order to investigate a terrorists activities and probably preventing terrorist attacks, the secret service needs to intercept and is also entitled to do so. The contextual integrity is **preserved**./ Alternatively (and maybe more plausibly), one might argue that no positive norm is fulfilled and that therefore, contextual integrity is **violated**. However, this would be a perfectly *justified* violation of privacy.

(f) **context:** Crime investigation
actors: everyone, involuntarily (sender), the secret service (information recipient), everyone (information subject)
attributes: everyone's communication
transmission principles: entitlement?
This might be rather a political question, but let us assume, that the secret service is not entitled to intercept the whole population (which is plausibly true). In this case no positive norm is fulfilled.
The contextual integrity is **violated**.

(e) and (f) are good examples of how it is not always clear which transmission principles hold in a situation.

Issue 6: ***Extra: Reading Nissenbaum***

Read the paper "Privacy and Contextual Integrity: Framework and Applications" by Barth et al., especially the first part up to page 9. How do you like the way that philosophy is combined with computer science here?