

Designing for Digital Transparency in the Public Realm:

Co-Design Workshop Material



This work is licensed by the Digital Transparency in the Public Realm project contributors, under a Creative Commons Attribution 4.0 International License.
<https://creativecommons.org/licenses/by/4.0/>

There's been a breach of the data that has been collected from one of these sensors – how does this impact what you need to know or do?

One of the sensors has been hacked – how should you know?

Should you be able to access data that's being collected around you? And if so, how should you be able to access it?

You disagree with how data is collected in this situation – what should you be able to do?

**How should you know if
the sensors in this situation
are being trialled?**

**Who should be accountable
for how the technology in this
situation works?**

**You want to check that the
sensors in this situation are secure
and the data is protected from
malicious actors – how should
you be able to do this?**

**Who should be accountable
for what is communicated
about the technology?**

Who or what should have oversight of how data in this situation is used?

How do you know that the data sharing agreements for how the data is used are being respected?

Who should set the permissions for how the data collected by these sensors is used and how should they do it?

Who benefits from the technology used in this situation?
Who doesn't benefit?

What if the data collected in this situation is cross-referenced with other data?

Who is responsible for maintaining the sensors used in this situation?

Who should make decisions about what data is collected in this situation and how it's used? Why?