Lesson 2

IRB：It’s still a grey area that Internet Experiment should be reviewed by IRB -> protect participants

Four Principles of IRB's

Ok, so we just went through some experiments that led to IRB’s being created. What are the four main principles that IRB’s look for?

First Principle: Risk

First, in the study, *what risk is the participant undertaking*? The main threshold is whether the risk exceeds that of “minimal risk”. Minimal risk is defined as the probability and magnitude of harm that a participant would encounter in normal daily life. The harm considered encompasses physical, psychological and emotional, social, and economic concerns. If the risk exceeds minimal risk, then informed consent is required. We’ll discuss informed consent further below.

In most, but not all, online experiments, it can certainly be debated as to whether any of the experiments lead to anything beyond minimal risk. What risk is a participant going to be exposed to if we change the ranking of courses on an educational site, or if we change the UI on an online game?

Exceptions would certainly be any websites or applications that are health or financial related. In the Facebook experiment, for example, it can be debated as to whether participants were really being exposed to anything beyond minimal risk: all items shown were going to be in their feed anyway, it’s only a question of whether removing some of the posts led to increased risk.

Second Principle: Benefits

Next, *what benefits might result from the study*? Even if the risk is minimal, how might the results help? In most online A/B testing, the benefits are around improving the product. In other social sciences, it is about understanding the human condition in ways that might help, for example in education and development. In medicine, the risks are often higher but the benefits are often around improved health outcomes.

It is important to be able to state what the benefit would be from completing the study.

Third Principle: Alternatives

Third, *what other choices do participants have*? For example, if you are testing out changes to a search engine, participants always have the choice to use another search engine. The main issue is that the fewer alternatives that participants have, the more issue that there is around coercion and whether participants really have a choice in whether to participate or not, and how that balances against the risks and benefits.

For example, in medical clinical trials testing out new drugs for cancer, given that the other main choice that most participants face is death, the risk allowable for participants, given informed consent, is quite high.

In online experiments, the issues to consider are what the other alternative services that a user might have, and what the switching costs might be, in terms of time, money, information, etc.

Fourth Principle: Data Sensitivity

Finally, *what data is being collected, and what is the expectation of privacy and confidentiality*? This last question is quite nuanced, encompassing numerous questions:

- Do participants understand what data is being collected about them?
- What harm would befall them should that data be made public?
- Would they expect that data to be considered private and confidential?

For example, if participants are being observed in a public setting (e.g., a football stadium), there is really no expectation of privacy. If the study is on existing public data, then there is also no expectation of further confidentiality.

If, however, new data is being gathered, then the questions come down to:

- What data is being gathered? How sensitive is it? Does it include financial and health data?
- Can the data being gathered be tied to the individual, i.e., is it considered personally identifiable?
- How is the data being handled, with what security? What level of confidentiality can participants expect?
- What harm would befall the individual should the data become public, where the harm would encompass health, psychological / emotional, social, and financial concerns?

For example, often times, collected data from observed “public” behavior, surveys, and interviews, if the data were not personally identifiable, would be considered exempt from IRB review (reference: NSF FAQ below).

To summarize, there are really three main issues with data collection with regards to experiments:

- For new data being collected and stored, how sensitive is the data and what are the internal safeguards for handling that data? E.g., what access controls are there, how are breaches to that security caught and managed, etc.?
- Then, for that data, how will it be used and how will participants' data be protected? How are participants guaranteed that their data, which was collected for use in the study, will not be used for some other purpose? This becomes more important as the sensitivity of the data increases.
- Finally, what data may be published more broadly, and does that introduce any additional risk to the participants?

Difference between pseudonymous and anonymous data

One question that frequently gets asked is what the difference is between identified, pseudonymous, and anonymous data is.

Identified data means that data is stored and collected with personally identifiable information. This can be names, IDs such as a social security number or driver's license ID, phone numbers, etc. HIPAA is a common standard, and that standard has 18 identifiers (see the Safe Harbor method) that it considers personally identifiable. Device id, such as a smartphone's device id, are considered personally identifiable in many instances.

Anonymous data means that data is stored and collected without any personally identifiable information. This data can be considered **pseudonymous** if it is stored with a randomly generated id such as a cookie that gets assigned on some event, such as the first time that a user goes to an app or website and does not have such an id stored.

In most cases, anonymous data still has time-stamps -- which is one of the HIPAA 18 identifiers. Why? Well, we need to distinguish between anonymous data and anonymized data. **Anonymized data** is identified or anonymous data that has been looked at and guaranteed in some way that the re-identification risk is low to non-existent, i.e., that given the data, it would be hard to impossible for someone to be able to figure out which individual this data refers to. Often times, this guarantee is done statistically, and looks at how many individuals would fall into every possible bucket (i.e., combination of values).

What this means is that anonymous data may still have high re-identification risk (see AOL example).

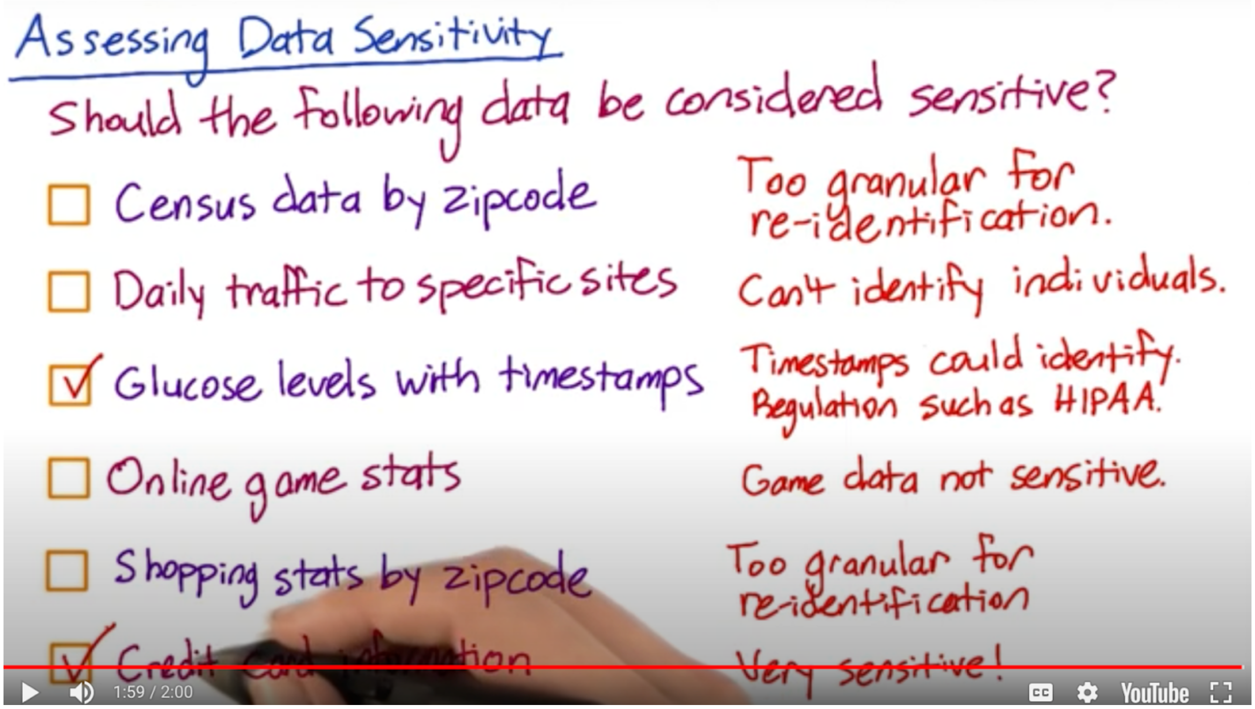
So, if we go back to the data being gathered, collected, stored, and used in the experiment, the questions are:

- How sensitive is the data?
- What is the re-identification risk of individuals from the data?

As the sensitivity and the risk increases, then the level of data protection must increase: confidentiality, access control, security, monitoring & auditing, etc.

Additional reading

Daniel Solove's "A Taxonomy of Privacy" classifies some of things people mean by privacy in order to better understand privacy violations.



Assessing Data Sensitivity

Should the following data be considered sensitive?

□ Census data by zipcode	Too granular for re-identification.
□ Daily traffic to specific sites	Can't identify individuals.
☑ Glucose levels with timestamps	Timestamps could identify. Regulation such as HIPAA.
□ Online game stats	Game data not sensitive.
□ Shopping stats by zipcode	Too granular for re-identification
☑ Credit card information	Very sensitive!

Summary of Principles

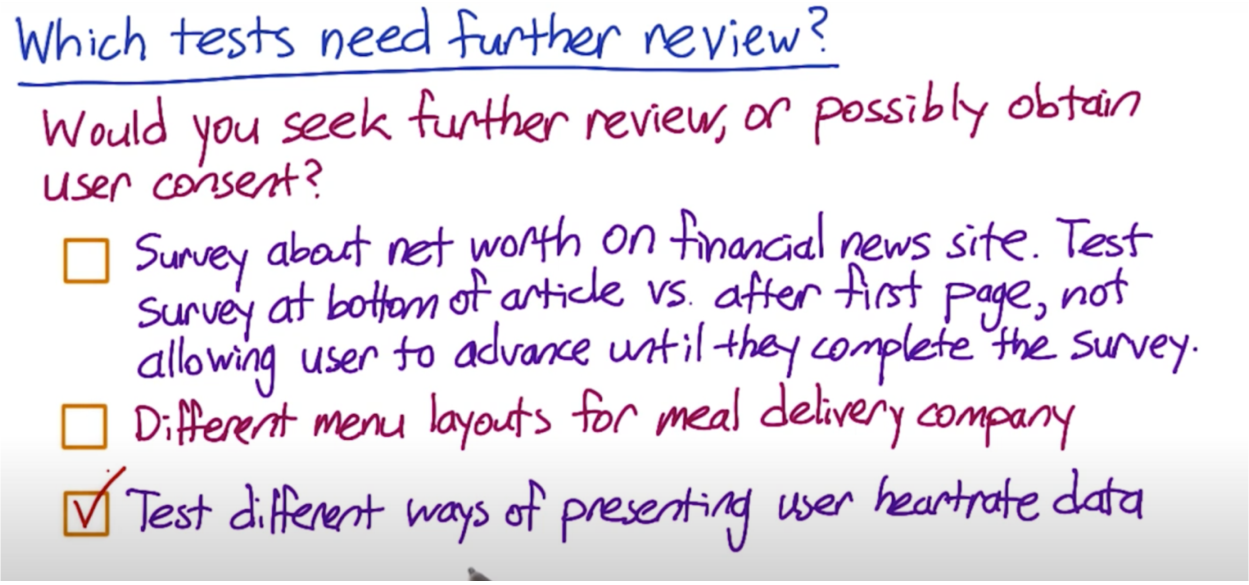
Summary: it is a grey area as to whether many of these Internet studies should be subject to IRB review or not and whether informed consent is required. Neither has been common to date.

Most studies, due to the nature of the online service, are likely minimal risk, and the bigger question is about data collection with regards to identifiability, privacy, and confidentiality / security. That said, arguably, a neutral third party outside of the company should be making these calls rather than someone with a vested interest in the outcome. One growing risk in online studies is that of bias and the potential for discrimination, such as differential pricing and whether that is discriminatory to a particular population for example. Discussing those types of biases is beyond the scope of this course.

Our recommendation is that there should be internal reviews of all proposed studies by experts regarding the questions:

- Are participants facing more than minimal risk?
- Do participants understand what data is being gathered?
- Is that data identifiable?
- How is the data handled?

And if enough flags are raised, that an external review happen.



Which tests need further review?

Would you seek further review, or possibly obtain user consent?

□ Survey about net worth on financial news site. Test survey at bottom of article vs. after first page, not allowing user to advance until they complete the survey.

□ Different menu layouts for meal delivery company

☑ Test different ways of presenting user heartrate data

Internal process recommendations

Finally, regarding internal process of data handling, we recommend that:

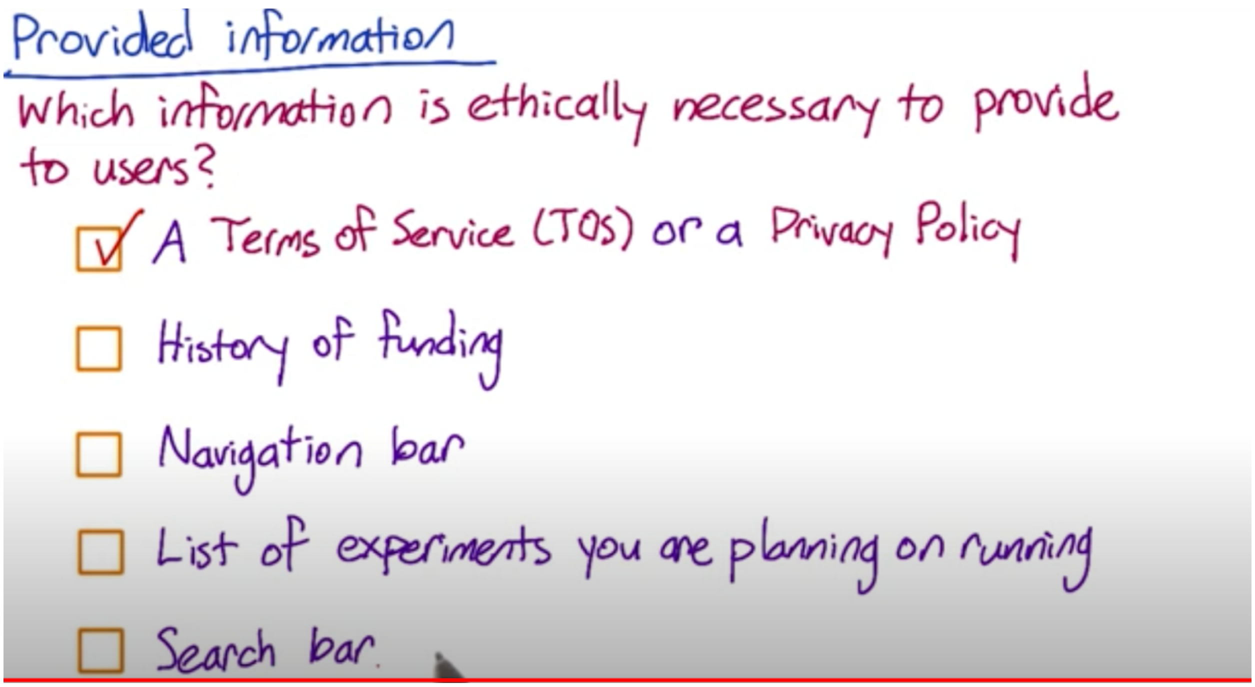
1. Every employee who might be involved in A/B test be educated about the ethics and the protection of the participants. Clearly there are other areas of ethics beyond what we've covered that discuss integrity, competence, and responsibility, but those

generally are broader than protecting participants of A/B tests (cite ACM code of ethics).

2. All data, identified or not, be stored securely, with access limited to those who need it to complete their job. Access should be time limited. There should be clear policies of what data usages are acceptable and not acceptable. Moreover, all usage of the data should be logged and audited regularly for violations.
3. You create a clear escalation path for how to handle cases where there is even possibly more than minimal risk or data sensitivity issues.

Additional reading:

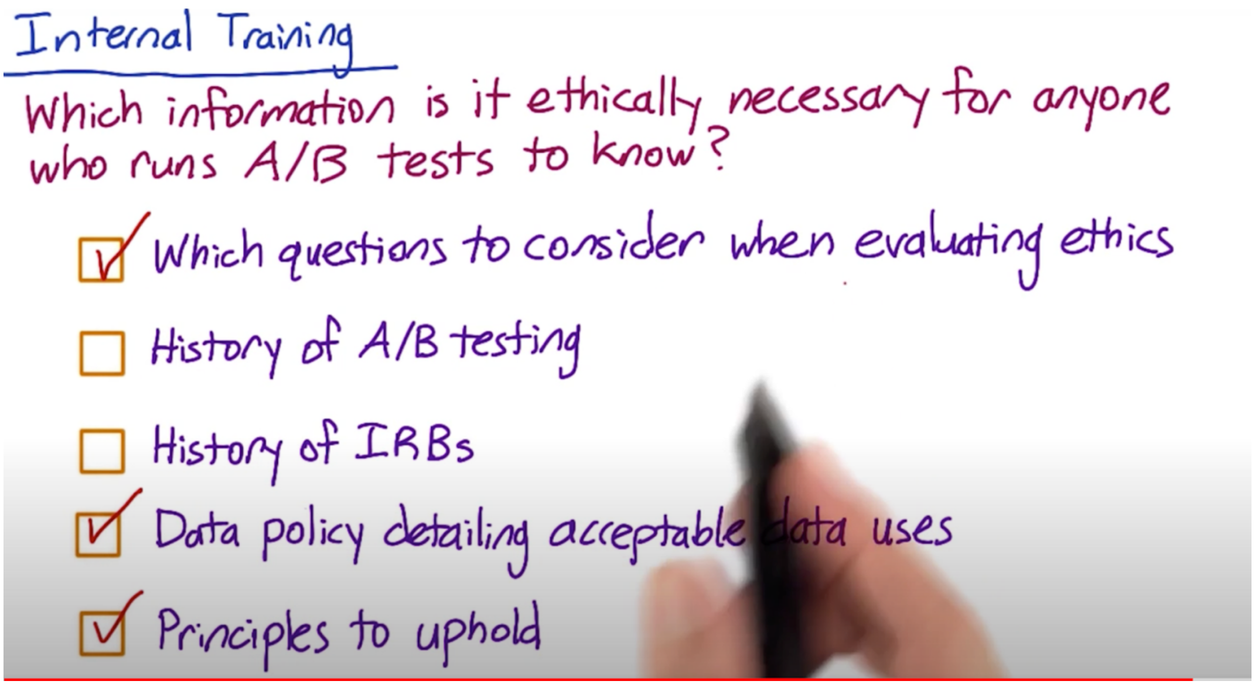
- Belmont Report
- Common Rule definition
- NSF guidelines
- NSF FAQ for Social Science & Behavioural research
- HHS IRB Guidebook
    - Definition of Minimal Risk
    - Discussion of different types of data gathering
- UTexas overview
- UC Irvine overview
- The Association for Computer Machinery has developed a code of ethics.
- As an example, there’s a thorough outline of an “ideal” ethical privacy design for mobile connectivity measurements that could be used as a model.



Provided information

Which information is ethically necessary to provide to users?

- ☑ A Terms of Service (TOS) or a Privacy Policy
- □ History of funding
- □ Navigation bar
- □ List of experiments you are planning on running
- □ Search bar



Internal Training

Which information is it ethically necessary for anyone who runs A/B tests to know?

- ☑ Which questions to consider when evaluating ethics
- □ History of A/B testing
- □ History of IRBs
- ☑ Data policy detailing acceptable data uses
- ☑ Principles to uphold