# Responsible Conduct of Research (RCR): Informed Consent

Emilee Rader
November 30, 2018

# The Belmont Report

- https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html
- Title is "Ethical Principles and Guidelines for the Protection of Human Subjects of Research”
- It was created in response to previous human subject violations
- It is the cornerstone of university IRBs (Institutional Review Boards)
- Three principles of ethical research:
  - Respect for persons
  - Beneficence
  - Justice

# Respect for Persons (1)

- Individuals should be treated as autonomous agents.
- An autonomous person is an individual capable of deliberation about personal goals and of acting under the direction of such deliberation.
- To respect autonomy is to give weight to autonomous persons' considered opinions and choices while refraining from obstructing their actions unless they are clearly detrimental to others.
- Persons with diminished autonomy are entitled to protection.

# Beneficence (2)

- Persons are treated in an ethical manner not only by respecting their decisions and protecting them from harm, but also by making efforts to secure their well being.
- "Do no harm" -- should not injure one person regardless of the benefits that might come to others.

# Justice (3)

- Who ought to receive the benefits of research and bear its burdens?

- An injustice occurs when some benefit to which a person is entitled is denied without good reason or when some burden is imposed unduly.

# Application of the principles from the Belmont Report: Informed Consent

# Informed consent (1) - Respect for Persons

- Participants must be given the opportunity to choose what shall or shall not happen to them. To that end, they must be told:
  - That the study involves research.
  - The purposes of the research.
  - They can voluntarily participate in the research study, can decline to participate, and can withdraw at any time for any reason after the study has started without penalty.
  - The risks, side effects or discomforts that might be reasonably expected.
  - Any benefits to themselves and others that can be reasonably expected.
  - The study's duration, what would happen in the study

# Informed consent (2) - Respect for Persons

- Participants must be given the opportunity to choose what shall or shall not happen to them. To that end, they must be told:
  - Appropriate alternative treatments that might be advantageous to the subject.
  - They may ask questions about the study before giving consent and at any time during the course of the study.
  - Allowed ample time, without pressure, to decide whether to consent or not to consent to participate.
  - Any treatments or compensation available if complications occur during the study.
  - The risk to the participant's privacy and confidentiality, an expiration date for the participant's authorization to use this information, and how to revoke authorization.

# Informed consent provides:

- An opportunity for choice…
- …before the study commences and any data are collected
- …based on honest and adequate information
- …allowing individuals to evaluate the risks and benefits
- …and decide for themselves whether they want to participate.
- Informed consent is not just a rule of the IRB — it is a moral obligation!
    - **What kinds of work do researchers need to do to meet this obligation?**

# How is Human Computer Interaction research unique?

- accessibility of venues and datasets means sometimes you work with data where you don't know what consent procedure was followed
- unobtrusive observation (lurking) makes online research attractive, but consent hard to obtain
- public vs. private spaces can be hard to differentiate, and IRBs have different consent rules for public or private observations
- when collecting log data, sometimes you don't know what measures you'll use until after you have the data, so it is hard to disclose how data will be used
- others???

# SCENARIOS

# Scenario 1

You're working on a research project investigating how people use the Internet to look up travel information. A lot of this happens via search engines, so you design a browser plugin to record users' search queries so that you can analyze them later. Your plugin also provides a side benefit to users: a visualization of all of their search queries. Somehow, your plugin becomes insanely popular, and during your study you collect search queries from millions of people. You make a point of obscuring the identities of your participants, identifying them only by a random number and not their name or other personal information. After you present your research, people start asking for access to your dataset for their own projects. You decide to release the data -- after all, it is anonymous, and data sharing is a Good Thing.

# Scenario 2

You have a project going on in which you're interested in how people share information about themselves in online medical forums, when they are going through a serious illness. You'd like to do some large-scale automated text data analysis to see if there are patterns for different circumstances in which people are more willing to share personal information in their forum posts -- perhaps when talking about how a particular drug worked for them, people might be more willing to share private medical information, than when offering messages of support to others. You sign up for an account on a forum website, and then use your new login credentials with a data scraper program you created to automatically download all of the forum posts going back as far as you can into the past. This is an explicit violation of the terms of service of the website, but you feel that there's no actual harm to the other users since it isn't that different from you just manually reading and downloading the information by hand.

# Scenario 3

You are working as a research assistant on a project funded by a popular social media platform. As part of the project, you spend a summer internship working for the company that operates the platform. During your internship, you help to design a new method to identify misinformation on the platform, by using machine learning techniques to pinpoint those users who are the most likely to spread misinformation. You also invent a “truth score”-based reputation system, so that others on the platform can stay informed about which other users they should be most skeptical of. After you return to your university, the method and accompanying user interface changes are implemented by the platform, and the platform operators conduct a study you helped to design, to measure how these changes affect peoples’ use of the platform. You plan to use this data about before vs. after changes as part of your dissertation research. It is exciting to not only be able to study such a hot topic, but also work with partners who have the ability to affect the lives of real people in such a positive way. You realize that this means there could be negative impacts for some of the users of the platform, but your industry partners assure you that informed consent just isn’t practical when operating at scale the way they do—it is impossible to get consent for every design change, after all.

# Scenario 4

It can be very hard in computer security research to figure out just *how much* of the internet is actually vulnerable to security risks. The internet is SO big, and it is organized in such a way that it is hard to get a representative sample. So, you decide to write a computer virus that only scans computers for vulnerabilities, reports what it finds, and then sends itself on to other computers. In that way it spreads like a regular computer virus, and is therefore able to get an interesting dataset for you to analyze. You don't want to actually harm anyone, so you build restrictions and limitations into your data collection virus about how many system resources it can take over to replicate itself, and how fast it can spread, to make sure that it doesn't adversely affect the computers it inhabits or the internet as a whole.

# Scenario 5

You are a researcher studying crisis informatics, focused on understanding how social media is used by people to share information and coordinate during large-scale emergency or crisis situations like wildfires, earthquakes, or floods. You build an application to record public tweets with certain words/hashtags in them, so that you can analyze them later for particular patterns of information dissemination. A terrorist attack occurs, and a manhunt ensues to track down and identify those responsible. Lots of information is shared back and forth as people re-examine photographs taken before the incident, report possible sightings, and re-post information from police scanners and "inside" sources. The suspect is apprehended, but not before an innocent person is mis-identified as the responsible party.

Later, you're analyzing the data you collected with your app, and you realize that it contains tweets posted or retweeted by certain key people with lots of followers that were instrumental in the mis-identification of an innocent person as a terrorist. You feel that this is quite interesting to study, and decide to write a paper about it -- after all, Twitter is public and these people knew what they were getting into when they posted the information.

# Scenario 6

People tend to be unwilling to self-report falling victim to a phishing attack, mostly because it is something people feel embarrassed and stupid about afterwards. This makes it hard to collect data about phishing -- you can't just ask people if it has ever happened to them, because they don't tell the truth. You're working on an important project to find out how likely people are to fall for phishing attacks, and you decide that the only way to answer this question is to send out realistic but "fake" phishing messages yourself and see if people fall for them. You take all of the necessary precautions to protect whatever sensitive, private data people reveal to you as part of the study. In addition, you don't want to make people feel bad or stupid as part of your study, and you want them to behave as they normally would when reading their email. So you argue to your IRB that you can’t get up-front consent, and even though your study involves deception, you don't think you should debrief afterwards either.