Lecture 24: Ethical Review of Research

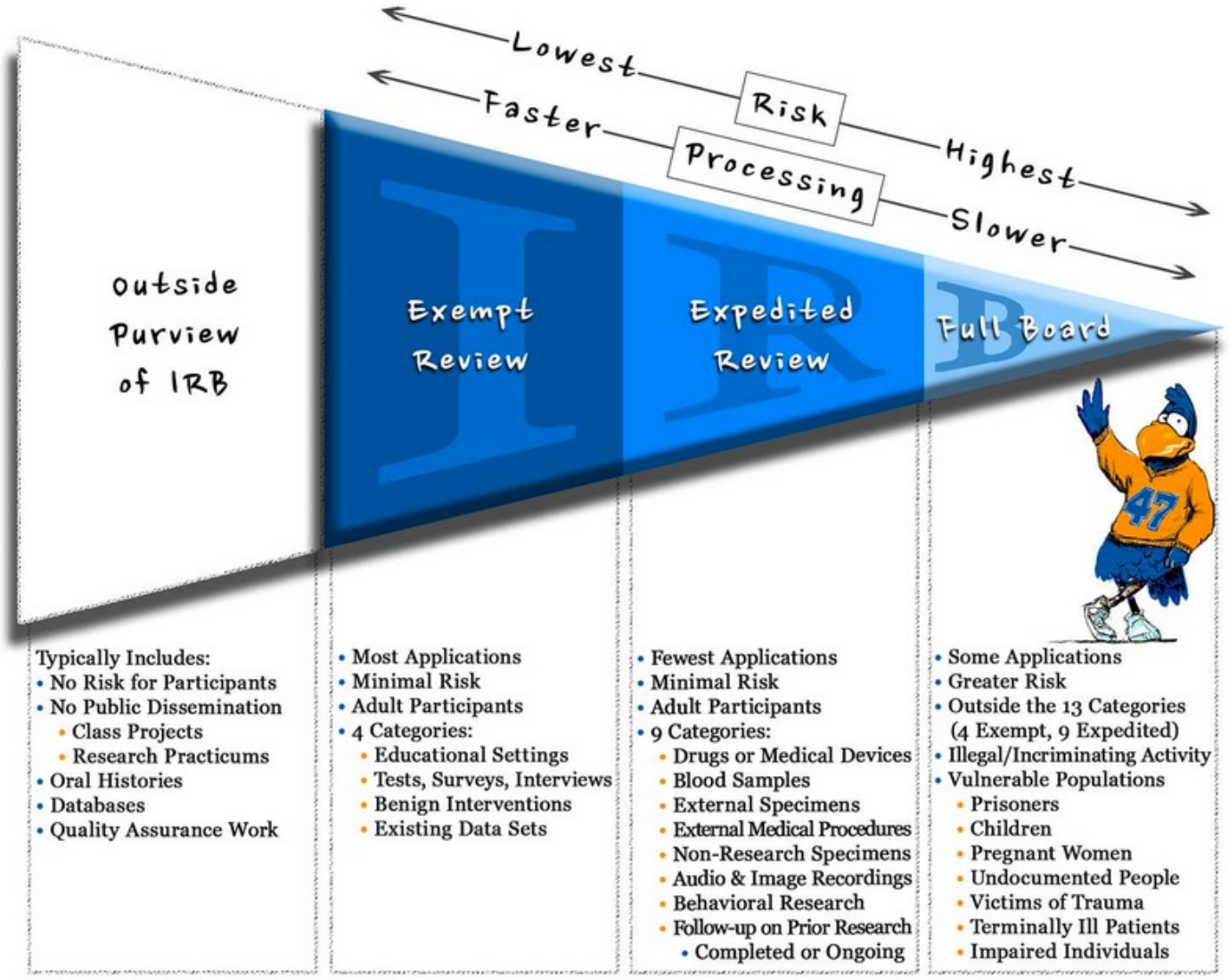
CS 181W

Fall 2022

Unethical Human Research

- Nazi biomedical experiments during WWII
- Tuskegee Study (1932-1972)
- Milgram experiment (1961)
- Stanford Prison Experiment (1971)

IRB Review

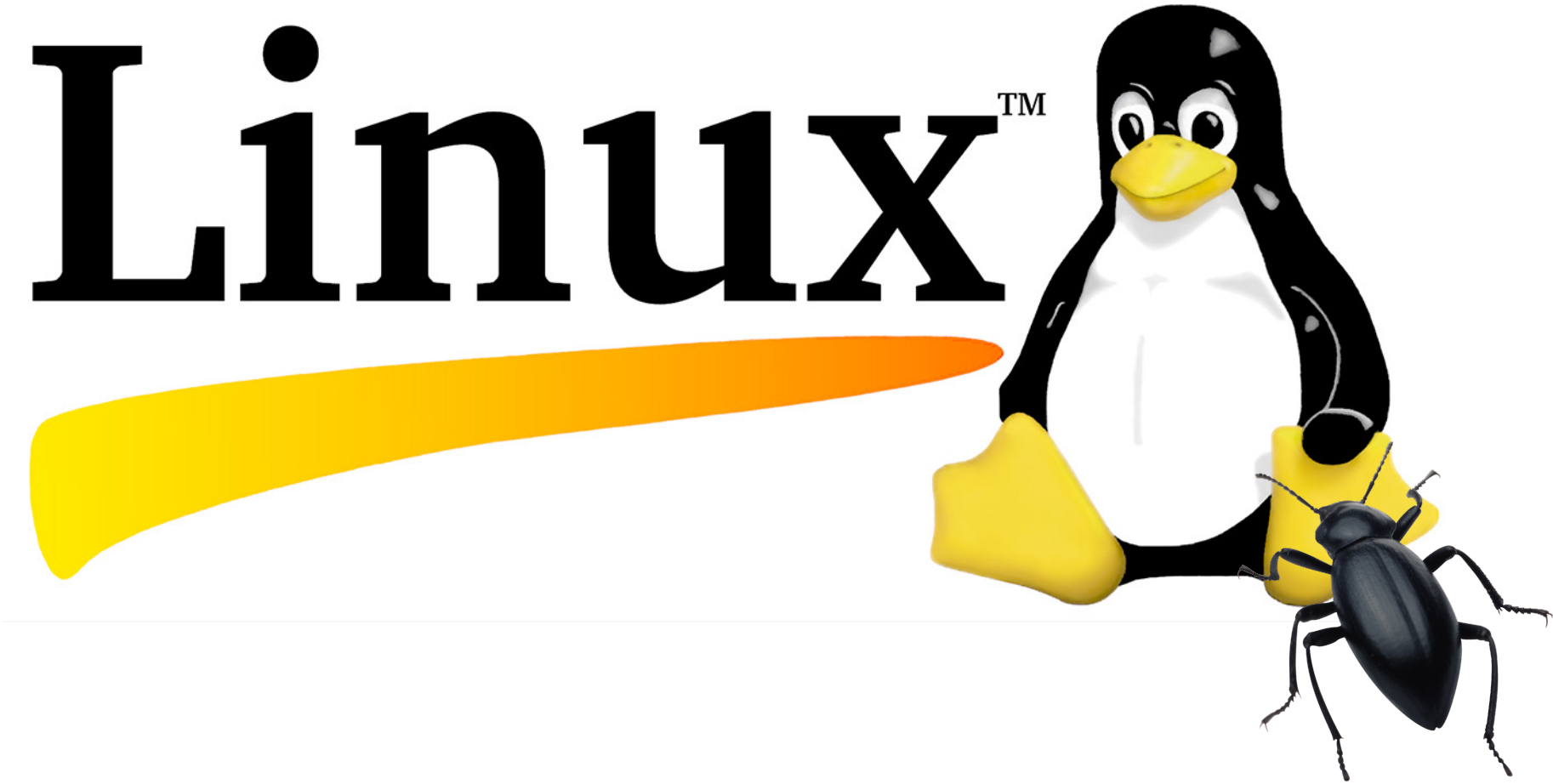

Lowest
Risk
Highest
Faster
Processing
Slower
Outside Purview of IRB
Exempt Review
Expedited Review
Full Board
Typically Includes:
• No Risk for Participants
• No Public Dissemination
◦ Class Projects
◦ Research Practicums
• Oral Histories
• Databases
• Quality Assurance Work
• Most Applications
• Minimal Risk
• Adult Participants
• 4 Categories:
◦ Educational Settings
◦ Tests, Surveys, Interviews
◦ Benign Interventions
◦ Existing Data Sets
• Fewest Applications
• Minimal Risk
• Adult Participants
• 9 Categories:
◦ Drugs or Medical Devices
◦ Blood Samples
◦ External Specimens
◦ External Medical Procedures
◦ Non-Research Specimens
◦ Audio & Image Recordings
◦ Behavioral Research
◦ Follow-up on Prior Research
• Completed or Ongoing
• Some Applications
• Greater Risk
• Outside the 13 Categories
(4 Exempt, 9 Expedited)
• Illegal/Incriminating Activity
• Vulnerable Populations
◦ Prisoners
◦ Children
◦ Pregnant Women
◦ Undocumented People
◦ Victims of Trauma
◦ Terminally Ill Patients
◦ Impaired Individuals

Common Rule

(e)(1) *Human subject* means a living individual about whom an investigator (whether professional or student) conducting research:

(i) Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or
(ii) Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

Example 1: Buggy Linux Updates



Example 2: Forged SAR emails

To Whom It May Concern:

My name is [Random Name], and I am a resident of [Random Location, often outside of the territorial jurisdiction of the referenced law]. I have a few questions about your process for responding to [Either CCPA or GDPR] data access requests:

1. Do you process [CCPA or GDPR] data access requests via email, a website, or telephone? If via a website, what is the URL I should go to?
2. What personal information do I have to submit for you to verify and process a [CCPA or GDPR] data access request? In particular, are there specific cookie values I should submit?
3. What information do you provide in response to a [CCPA or GDPR] data access request? In particular, would you provide records of my activity on websites other than your own?

To be clear, I am not submitting a data access request at this time. My questions are about your process for when I do submit a request.

Thank you in advance for your answers to these questions. If there is a better contact for processing [CCPA or GDPR] requests regarding [Some URL, often not associated with the receiving company], I kindly ask that you forward my request to them.

I look forward to your reply without undue delay and at most within [45 days o 1 month], as required by [CCPA or GDPR legal reference].

Sincerely,

[Random Name]

- Goal: study how websites implement data rights
- forged requests sent to thousands of top websites

Example 3: Pseudo SAR Emails

To whom it may concern,

My name is [profile pseudonym] and I am writing to request access to my data as provided under CCPA. Specifically, I am requesting the following information:

1. Specific pieces and categories of personal information requested, collected, and shared by [the app]
2. Categories of sources from which my personal information was collected
3. Your purposes for collecting my personal information
4. Specific names and categories of third parties with whom you shared my personal information

If you need any further information to process my request, please let me know.

Sincerely,
[profile pseudonym]

- Goal: study how mobile apps implement data access rights
- CA researchers created fake profiles
- sent SARs to top mobile apps for data associated with those fake IDs
- restricted to apps that mentioned CCPA in policy

Discussion Questions

What constitutes human subject research (in the context of security and privacy)?

What constitutes ethical research (in the context of security and privacy)?

What research should be subject to advance ethical review by an external reviewer (e.g., IRB review)?

Ethical Review of Research