Questions to Consider

- Can you justify building a re-identification technology based on the fact that someone else might build it?
- Can you justify dissemination of a re-identification technology based on your intent to promote the strengthening of existing privacy protections?
  - "disseminate" can mean many different things
- How can we reason about these concerns?

Do No Harm?

- Hippocratic Oath
  - CONFIDENTIALITY: “Whatever in connection with my professional practice or not in connection with it I may see or hear in the lives of my patients which ought not be spoken abroad, I will not divulge, reckoning that all such should be kept secret.”
  - DO NO HARM: “Except for the prudent correction of an imminent danger, I will neither treat any patient nor carry out any research on any human being without the valid informed consent of the subject or the appropriate legal protector thereof, understanding that research must have as its purpose the furtherance of the health of that individual. Into whatever patient setting I enter…”

Secondary Data Landscape

- No direct involvement with patients, only their information
- Information may be shared with restrictions (Limited Data Sets), but may also be publicly available
  - Census
  - National Center for Biotechnology Information

Harm?

- Is your intent of harm justified if the publication of personal data was not based on an intent of harm?
- Are you putting people in unnecessary harm?
- Should you publish technology that exposes vulnerability when there is no means for protection?

Outline

- Construction and Use of Disruptive Technologies
- Ethical Reasoning
- Containment and Limits of Research
- Dual-Use
July 16, 1945

- First nuclear detonation
- Alamogordo, NM
  - "Trinity" test
- Manhattan Project
- Fears over Nazi development of an atomic bomb
- Employed 130,000 people
- $2 billion dollars invested in project development

August 6, 1945
Hiroshima

August 9, 1945
Nagasaki

July 9, 1955

- "We appeal as human beings to human beings: Remember your humanity, and forget the rest. If you can do so, the way lies open to a new Paradise; if you cannot, there lies before you the risk of universal death."
  -- Russell-Einstein Manifesto
- Signed by Max Born (1914), Percy Bridgman (1946), Leopold Infeld, Frederic Joliot-Curie (1935), Herman Muller (1946), Linus Pauling (1954), Cecil Powell (1950), Joseph Rotblat, and Hideki Yukawa (1949)
- Called Congress & scientists to assemble and discuss the threat posed by thermonuclear weapons
  - Regardless of political persuasion

1957

- Guest lodge of Cyrus Eaton
- Pugwash, Nova Scotia
- Attendance of 22 international scientists
  - 7 from USA
  - 3 from Japan, USSR
  - 2 from UK, Canada
  - 1 from Australia, China, France, Poland

Pugwash Activities

- "Channel of communication between scientists, scholars, and individuals experienced in government, diplomacy, and the military
- for in-depth discussion and analysis of the problems and opportunities at the intersection of science and world affairs."
- "All participants in Pugwash activities are individually invited by the Pugwash Council."

Pugwash

- 1995 – awarded the Nobel Peace Prize (with Rotblat)
  - "for their efforts to diminish the part played by nuclear arms in international politics and, in the longer run, to eliminate such arms."
- But so much more
  - Conferences on biological weapons, nuclear weapons, chemical weapons, sustainable development and the environment, artificial intelligence, robotics
- Senior level ⇐ closed meetings
- Student level

http://www.pugwash.org
Take Home Message

- Scientists must go **beyond** their science
- It is your **responsibility** to recognize the potential for threats to humanity

Outline

- Construction and Use of Disruptive Technologies
- Ethical Reasoning
- Containment and Limits of Research
- Dual-Use
- Ethical (?) Hacking
- Technology, Policy, & Ethics

Ethical Reasoning

- Process to ensure actions are justifiable according to general standardized principles, rather than the issues of the moment
- Focus on foresight, as opposed to hindsight
- Three Steps
  1. Be aware of differing ethical codes
  2. Identify key facts that impact decision situation
  3. Logical application of chosen ethical code
     - Draw conclusion based on an ethical, and logical, course of action
     - Choose the course

Ethical Reasoning

- Consequentialist
  - Choose the action with the best overall consequences
  - Morally right if the act, or motive, is chosen only with consideration for the consequence
  - "The ends justify the means"
  - Discounts the treatment of people and actions
- Obligationist
  - Certain actions are inherently right or wrong
  - Do not balance the consequences to determine obligations

Some Ethical Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Model</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilitarianism</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Some Ethical Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Model</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilitarianism</td>
<td>Choose action that maximizes the good for the greatest number of people</td>
<td>Consequentialist</td>
</tr>
<tr>
<td>Universal Application Code</td>
<td>Action is “right” if everyone accepts the moral rule presupposed by the action</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Golden Rule</td>
<td>Reciprocity - “Do unto others as you’d have done to you”</td>
<td>Obligationist</td>
</tr>
</tbody>
</table>

**Utilitarianism**

Choose action that maximizes the good for the greatest number of people

**Consequentialist**

Action is “right” if everyone accepts the moral rule presupposed by the action

**Obligationist**

Reciprocity - “Do unto others as you’d have done to you”
### Some Ethical Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Model</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilitarian</td>
<td>Choose action that maximizes the good for the greatest number of people</td>
<td>Consequentialist</td>
</tr>
<tr>
<td>Universal Application Code</td>
<td>Action is &quot;right&quot; if everyone accepts the moral rule presupposed by the action</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Golden Rule</td>
<td>Reciprocity - &quot;Do unto others as you'd have done to you.&quot;</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Human Rights</td>
<td>Respect the rights of others (i.e., right to life, safety, privacy, etc.)</td>
<td>Obligationist</td>
</tr>
</tbody>
</table>

### Human Rights

- Respect the rights of others (i.e., right to life, safety, privacy, etc.)

### Natural Law

- Action is "right" if legitimate authority says it is (legislative body, professional society) "right"
### Some Ethical Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Model</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilitarianism</td>
<td>Choose action that maximizes the good for the greatest number of people</td>
<td>Consequentialist</td>
</tr>
<tr>
<td>Universal Application Code</td>
<td>Action is “right” if everyone accepts the moral rule presupposed by the action</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Golden Rule</td>
<td>Reciprocity: “Do unto others as you’d have done to you”</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Human Rights</td>
<td>Respect the rights of others (i.e., right to life, safety, privacy, etc.)</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Natural Law</td>
<td>Action is “right” if it is good for the greatest number of people</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Computer Ethics Institute</td>
<td>10 commandments for computer use</td>
<td>Obligationist</td>
</tr>
</tbody>
</table>

### Some Ethical Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Model</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilitarianism</td>
<td>Choose action that maximizes the good for the greatest number of people</td>
<td>Consequentialist</td>
</tr>
<tr>
<td>Universal Application Code</td>
<td>Action is “right” if everyone accepts the moral rule presupposed by the action</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Golden Rule</td>
<td>Reciprocity: “Do unto others as you’d have done to you”</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Human Rights</td>
<td>Respect the rights of others (i.e., right to life, safety, privacy, etc.)</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Natural Law</td>
<td>Action is “right” if it is good for the greatest number of people</td>
<td>Obligationist</td>
</tr>
<tr>
<td>Computer Ethics Institute</td>
<td>10 commandments for computer use</td>
<td>Obligationist</td>
</tr>
</tbody>
</table>

### Computer Ethics Institute

- Began as a project of the Brookings Institute
- Don’t use a computer to harm other people
- Don’t interfere with other people’s computer work
- Don’t snoop around in other people’s computer files
- Don’t use a computer to steal
- Don’t use a computer to bear false witness
- Don’t copy or use proprietary software for which you have not paid
- Don’t use other people’s computer resources without authorization or proper compensation
- Don’t appropriate other people’s intellectual output
- Think about the social consequences of the program you are writing or the system you are designing
- Always use a computer in ways that Insure consideration and respect for your fellow humans

---

### Utilitarianism

- Dates to Epicurus (~300 BC)
- Formalized by Bentham
  - “The greatest happiness principle” (a.k.a. “the principle of utility”)
  - Term attributed to David Hume
  - Evaluation of actions based on their consequences
  - Actions that do not maximize the greatest happiness are considered morally wrong
- Popularized by Mill
  - Actions rooted in self-interest
  - Personal feelings often conflict with self-interest, but they are contrary to pleasure

---

### Jeremy Bentham

| (1748 – 1832) |

---

### John Stuart Mill

| (1806 – 1873) |
Utilitarianism - Problems
- If everyone acts in pure self-interest, there is a potential for suboptimal results
- Tragedy of the Commons
  - Limited resources
  - Each action has a positive and negative component
    - Positive – personal benefit by consuming resource
    - Negative – less resource available
  - At any particular point in time, personal gain outweighs the personal share of distributed cost
  - Overuse of resources


Utilitarianism Relaxed
- Some people must lose so that others may benefit
- Challenge is in defining “utility”
  - Everyone may have a different notion of what is “best”


Principle of Double Effect
- A.k.a. Doctrine of Double Effect
- Attributed to St. Thomas Aquinas
  - Italian Catholic philosopher and theologian
- System of ethics
  - Rooted in Aristotle reasoning
  - Will willed the end, it also willed the appropriate means – chosen freely
  - Man’s will is an inclination toward universal good
  - In a chain of acts, man strives toward the highest end
  - Free acts, such that man has knowledge of their end
  - If an act is “good” or “evil” depends on the end

A. K. Thomae Aquinæs (1225 – 1275)

Principle of Double Effect
- Certain actions have multiple effects
- Special case – two effects
  - Good effect: Result is positive benefit for the recipient
  - Bad effect: Result is a negative cost for the recipient
  - Do not necessarily observe both the good and bad effects

St. Thomas Aquinas (1225 – 1275)

Principle of Double Effect
- Four (sometimes five) conditions
  - Primary Four
    1. The act’s nature is morally neutral (or positive)
    2. Intent of the actor is for the good, not the bad, effect
    3. Good effect outweighs the bad effect in a situation sufficiently grave to merit the risk of generating the bad effect
    4. Good effect does not proceed through the bad effect
    5. From a causal perspective, the bad effect is no closer to the act than the good effect

Summary of Principle
The entity initiating the action can not inflict harm to achieve good.

Note, this does not imply there are no harms that manifest as a bi-product.
Moral Neutrality

- An entity or object that has no intent regarding its action
- A tool, such as a screwdriver, can be used in either a morally defensible or morally problematic way
- If a pillowcase is used by a perpetrator for suffocation, the pillowcase did not intend the harm.
- That said, are all technologies morally neutral?

Example

- Pharmaceutical manufacturer knows
  - Good: drug X will save lives ← Intended result
  - Evil: some people may die as a side effect of drug X
- Pharmaceutical is “morally neutral”
- Lives are saved as a result of the drug, not the deaths
- The evil effect does not further the manufacturer’s goals
  - Evil effect is not the means
- If number of lives saved >> than number of lives lost, then the set of actions satisfies the proportion condition

Double Effect Visual

Unacceptable – But Not Bad

Unacceptable

Unacceptable

Good and Evil acts are not always independent.
Unacceptable

Actor’s Intent

Act

P(G | Act, no E)
P(G | Act, E)

Good Result

Person

P(G | Act, E)

Evil Result

P(G | Act, no E)

P(G | Act, no E) ≤ P(G | Act, E)

Re-identification from Double Effect Perspective

Actor’s Intent

Act

P(G | Act)
P(E | Act)

Good Result

Person

Morrally Neutral

P(G | Act)
P(E | Act)

Evil Result

Does this Make Sense?

- Consequentialists often take issue with the idea that two actions can differ in acceptance if they have the same consequences
- What about the case where some evil must be knowingly done to bring about an overwhelming quantity of good
  - E.g., re-identification of 1,000,000 records to prove to company that the threat to their records is real
  - E.g., exposure of a single re-identification to convince a company that the threat to 1,000,000 records is real

So?

- Ok, so you’ve constructed your models and scenarios, weighed your probabilities, and you can justify your actions
- You do not live in a bubble

Outline

- Construction and Use of Disruptive Technologies
- Ethical Reasoning
- Containment and Limits of Research
- Dual-Use

Asilomar (mid-1970’s)

- 1972 – Recombinant DNA technology
  - Paul Berg splices monkey virus SV40
  - Merges it with lambda bacteriophage
  - (stops there, but intention for the following)
  - Infect E. coli with bacteriophage
  - Recombine bacterial DNA
- Asilomar Conference on Recombinant DNA
  - Scientists (mainly biologists), lawyers, physicians
  - Concern about biohazard
  - Establish principles on how to handle experimental design
Assilomar Recommendations

1. Containment, containment, containment
2. Dock containment to risk level
   1. Low: experiment generates a novel biospecimen, but recombinant DNA does not have minimal impact on behavior of the recipient species, pathogenicity, or effective treatments of infections
   2. Moderate: probability of significant pathogenicity or behavioral disruption
   3. High: potential for serious biohazard to laboratory personnel or to the public
3. Biological barriers: biological strains that would have trouble surviving beyond the lab
4. Physical containment of biospecimens
5. Education and training of all personnel

Prohibited Experiments

- Cloning of recombinant DNA derived from highly pathogenic organisms
- Cloning of DNA containing toxin genes
- Large scale experiments to synthesize products that were harmful to animals and plants
- Participants avoided strict legislative recommendations for fear of limiting scientific progress / creativity

Analogy

- To what extent are information technologies like biotechnologies?
  - Materials
  - Economics
  - Expertise
  - Regulatory

Outline

- Construction and Use of Disruptive Technologies
- Ethical Reasoning
- Containment and Limits of Research
- Dual-Use
- Ethical (?) Hacking [held over for later]
- Technology, Policy, & Ethics [held over for later]

Dual-Use

- Research / Artifacts with the potential for
  - Valuable scientific knowledge
  - “nefarious” purposes

Dual-Use History

- Originally from the military
- Dual-Use technology: something that could be used in peacetime and war
- Example: Nuclear technologies
  - Reactors vs. bombs
- Example: In 2002, researchers at SUNY Stony Brook synthesized live polio viruses
  - Pieced together DNA fragments into polio virus “template”
Dual-Use Principles

- Identify primary-use and dual-use
- Identify potential for dual-use risk
- Identify magnitude of dual-use event
- Identify reach of dual-use

- Can dual-use be characterized using simulated data?
  - For instance, is it sufficient to investigate the uniqueness of de-identified data (assuming that a linkage model exists)

Dual Use In Infrastructure

- Development of dual-use technologies falls under
  - vulnerability analysis for critical infrastructure
  - possible warning or response …
  - but re-identification doesn’t necessarily have a clear response

Critical Infrastructure Protection

- Vulnerability Analysis
  - For each sector of the economy / government
  - Rank risk and threat
- Remedial plan
  - timeliness, implementation, responsibilities, & funding
- Warning
  - National center to detect, analyze, and warn of significant infrastructure attacks
- Response
  - building and minimizing damage
- Reconstruction
  - Rapid rebuild of minimum required capabilities
- Education and Awareness
  - Sensitive people to importance of security and train them in standards – particularly with regard to cyber systems
- Research & Development
  - Federal and private funding to support infrastructure protection
- Intelligence
  - Intelligence Community enhance collection and analysis of foreign threats
- International Cooperation
  - At government and corporate levels
- Legislative and Budgetary Requirements
  - Evaluate existing laws, regulations, and support for each of the previous tasks

Fink Report

- Response to threats generated by biological research
  - Public health & national security
  - Chaired by Gerald Fink (MIT / Whitehead molecular biologist)
  - Experts from microbiology, public policy, biomedical ethics
- Published “Biotechnology Research in an Age of Terrorism” (a.k.a. Fink Report) in 2004
  - National security + life sciences
  - “dual use dilemma” in the life sciences
  - 7 classes of “experiments of concern” that were considered the most risky in context of misuse threat
  - Recommended establishment of a federal advisory committee
- Provide guidance on biosecurity vs. biodefense

Experiments of Concern

1. Demonstrate how to render a vaccine ineffective
2. Confer resistance to antibiotics or antivirals
3. Enhance a pathogen’s virulence or render a non-pathogen virulent
4. Increase a pathogen’s transmissibility
5. Alter a pathogen’s host range
6. Enable evasion of diagnostic tests
7. Enable weaponization of pathogens and toxins

Analogies

- Vaccine \(\rightarrow\) Method / Agent to protect data before it is discovered
- Anti-(biotic, viral) \(\rightarrow\) Method / Agent to protect data after potential compromise
- Pathogen \(\rightarrow\) Method / Agent by which privacy is compromised
- Diagnostic \(\rightarrow\) Method / Agent by which privacy compromise is detected
- Weaponization \(\rightarrow\) Migration from “technology is neutral” towards “technology with malicious intent”
Consider in Re-identification Context

- Demonstrate how to render a vaccine ineffective
  - Demonstrate how to render identity protection ineffective (protection function / algorithm)
  - Confer resistance to antibiotics or antivirals
    - Prevent protection of identity misuse after it has been compromised (e.g., blackmail, identity theft, insurance discrimination, keeping datasets online in perpetuity)
- Enhance a pathogen’s virulence or render a non-pathogen virulent
  - Make a re-identification attack stronger (e.g., make algorithms more robust; make re-identification attack more specific → 5 instead of 10 people)
  - Adapt an existing record linkage package (e.g., FEBRL) for re-identification purposes

Consider in Re-identification Context

- Increase a pathogen’s transmissibility
  - Provide a means for allowing others to conduct or view the results of re-identification
    - Publication of methodology
    - Publication of <name, sensitive data> results
- Alter a pathogen’s host range
  - Use re-identification technique to infer / link to confidential information (this is a data privacy concern beyond compromise of anonymity, this is compromise of private information)
  - Adapt a re-identification technique for a new population (e.g., originally designed for Tennessee → adaption for Arkansas)

Consider in Re-identification Context

- Enable evasion of diagnostic tests
  - Prevent others from determining if re-identification can occur (e.g., an insurance company refuses to disclose the information it holds on the population; hospital refuses to disclose information to discharge database → thus the hospital maintains private information it can leverage for re-identification of others’ datasets)
- Enable weaponization of pathogens and toxins
  - Linking your re-identification software to credit card applications
  - Selling your re-identification software to home loan agency (identification of cancer patients)
  - Making your software freely available online

Consider in Re-identification Context

- Experimental design changes to mitigate dual-use risk, include
  - Substitution of marker protein for a toxin in a proof-of-concept experiment
  - Replacement of virulent microbe with an attenuated strain to obtain information
- Some projects altered, but none have been halted and no publications stopped
- Institutional biosafety committees (IBC)

Risk Identification

- National Science Advisory Board for Biosafety (NSABB) recommends dual-use risk be identified by investigator
- Not enough
  - Policy-makers and administrators should provide researchers
    - with information to enable discovery of concerns
    - Draft mechanisms to address problems when discovered

Options

- Oversight agency
  - Southeast Regional Center of Excellence for Biodefense and Emerging Infections (SERCEB)
- Policy, Ethics, & Law (PEL) recommendation
  - Defer publication, or publication plans, until discussion with steering committee
  - Works well for biological agents, but what if no such committee exists? What about information technology?
- PEL favors modification of results
  - Similar to a “attenuation” biological / technological
When Do You Hide Information?

**BENEFITS**

**RISKS**

- What are the goals for development / publication?
- Can these goals be achieved through another route?
- Competing issue: funding agencies

Outline

- Construction and Use of Disruptive Technologies
- Ethical Reasoning
- Containment and Limits of Research
- Dual-Use