The Future of the Internet--And How to Stop It
(Jonathan Zittrain)

John Banya and Brandon Botsch
Subject Matter Overview

- **Generative**: Open systems that “foster the production of useful things” and allow people to express themselves.
  - Pro: Allows users to experiment and create new technology.
  - Con: Allows for malicious use and are not reliable.

- **Sterile (Appliancized)**: Closed systems that are managed by a central authority that do not allow outside influences or experimentation.
  - Pro: Easy to use (typically designed for limited purposes) and safe.
  - Con: Prevents creativity and changes from external users. Harder to enforce privacy. Leaves user information subject to the will of companies.

- **The Generative Pattern**: New “generative” ideas and technologies follow a recurring pattern from conception to growth to inevitable exploitation.
Summary - History

- Early “computing” technology competed between generative and appliancized.
  - Personal Computers (generative) vs. IBM Mainframes (appliancized)
  - Internet (generative) vs. CompuServe (appliancized)
  - Wikipedia (generative) vs Encyclopedia Britannica (appliancized)
- Generative technology emerged as the victor over appliancized technology.
  - E.g. Internet became more popular than subscription-based private networks (i.e. CompuServe).
  - Generative technology allows users to create and implement new ideas without approval from a bureaucracy.
  - Procrastination Principle: “invitation to others to overcome the [...] shortcomings, and to continue adding to its uses”.
- Generative technology is inherently less secure and stable.
  - Appliancized technology seeing a resurgence.
Summary - Problems

- Internet initially built under the assumption that users will be “good”.
  - Initially used by universities and government.
  - Was built to be as simple and transparent as possible (just passes packets and nothing else).
- Viruses/Malware
  - Internet’s generativity easily allowed the creation of viruses and other malicious software that spread throughout the network.
- Copyright
  - Internet’s ability to share information freely leads to issues of copyrighted material being distributed.
- Criminal Activity
  - Internet’s low barrier of entry and ease of use enables criminal activity such as child pornography to proliferate.
- Privacy
  - Generative nature of the Internet creates a new class of privacy issues not previously encountered
Summary - Solutions

- **Applicanization.**
  - Leave control in the hands of the manufacturer.

- **Give users a shared stake in what occurs elsewhere online.**
  - Create tools that allow collaboration on determining the safety of new software (e.g. Web of Trust)

- **Network Defenses**
  - Urge ISPs to filter threats at the network level rather than deferring defenses to end-users.

- **Create entities to fight malicious websites.**
  - E.g. StopBadware - Find and mark bad websites on Google.

- **Clarify copyright laws**
  - Modify statute of limitations and improve legal uncertainties.
  - Hold individual wrongdoers accountable for their actions (e.g. create ways of identifying people).

- **Give users more privacy options**
  - Create standards (like robots.txt) to prevent privacy infractions.
  - Give users the ability to correct information about themselves online.
Points of Agreement with Class

- Constitutional Issues
  - 4th Amendment - Applies to data store locally on PC, but not to data stored in online services
  - 1st Amendment - The “Libertarian gotcha” to authoritarian regimes: if one wants technological progress and the associated economic benefits, one must be prepared to accept some measure of social liberalization made possible with that technology.

- Government Surveillance and Secondary Use
  - “Entrusting information to third parties changes the ease of surveillance because those third parties are often willing to give it up”
  - Government can demand data stored about users from private companies.
  - Government can demand that companies install surveillance software on their manufactured devices (e.g. OnStar)
Points of Agreement with Class

● “Chilling Effect”
  ○ Widespread availability of cameras means anybody can record anyone else in public.
  ○ Potential for spreading of private information from public or semi-public places creates a “chilling effect”.

● The Code of Fair Information Practices
  ○ Written in 1973 and only applies to government data collection, not to companies.
  ○ Much more difficult to enforce on the entire Internet because of the amount of information.
  ○ Less relevant today because people often willingly give up their data.
  ○ “When many of us maintain records [...] through peer-produced social networking services [...] then exactly what the database is changes from one moment to the next--not simply in terms of its contents, but its very structure and scope. Such databases may be generally unknown while not truly ‘secret’”
Going Beyond

- Privacy 1.0 vs Privacy 2.0
  - Privacy 1.0 refers to the traditional threats to privacy associated with government and corporate databases
  - Privacy 2.0 refers to the emergence of new privacy threats coming out of the generative Internet as a result of interpersonal interaction.
  - People now giving up so much of their data out of convenience creating a much greater pool of information.
  - “The essence of Privacy 2.0 is that government or corporations, or other intermediaries, need not be the source of the surveillance.”
Differing Viewpoints from Class

- Less law, more “standards”
  - Zittrain argues less for a law-based approach and more for universally agreed upon standards.
  - “A small lesson of the [stop-sign-less] experiment is that the standards can work better than rules in unexpected contexts [...] When we face heavy regulation, we see and shape our behavior more in relation to reward and punishment [...] than because of a commitment to the kind of world our actions can help bring about.”

- Solutions for problems in modern-day privacy are different from traditional remedies.
  - “Effective solutions for the problems of Privacy 2.0 may have more in common with the solutions to other generative problems than with the remedies associated with the decades-old analytic template for Privacy 1.0”
  - We may need to investigate new methods of enforcing privacy.

- Link personal identities to ones used online
  - “When we participate in other walks of life [...] we do so as ourselves [...] The same should be possible for our online selves.”
  - Allow information to be linked against real people, who can then have options to delete old information.
  - May be necessary to give up some privacy to enforce other forms of privacy.