Topic: Hacktivism and Whistleblowers

General vocabulary:

- Hacking-related nouns: Fraud, malware, vulnerability, flaw, scam, privacy, security, threat
- Hacking-related verbs: Disclose, expose, uncover, disable
- Miscellaneous terms associated with hacktivism: Anonymous, illegitimate, anti-establishment

Cartoons:
https://64.media.tumblr.com/tumblr_m4mzs8OUD41rscu8qo1_640.gifv

What are the opinions of the people who likely created this?

Questions:

Who hacktivists are and what they stand for

- Are people who hack computer systems criminals? Why or why not and when? (One point in their favor: They can, in some cases, expose vulnerabilities and push Internet sites to innovate and become better and stronger.)
- Are they promoting freedom of information?
- What kind of risks do hacktivists take?
- Should hackers be given more freedom? What are the pros and cons of doing this?
- Should computer geniuses who want to help join internet technology firms instead of breaking into whatever systems they want? Would they be able to help this way? (One possible solution: They could be hired as independent consultants to find vulnerabilities, since people within an organization often don't see its flaws.)

How hacktivists may or may not contribute to a cause

- Do hacktivists mainly fight for data-related causes?
- Can they be just as effective as activists?
- Could hacktivism start a movement or just contribute to existing ones?
- Do you think hacktivists are contributing to peoples' lives in any way?
- Can hacktivists be taken seriously by the general public? Would you? Why or why not?

Hacktivists and government

- Do hacktivists help us by fighting large government organizations that invade our privacy?
- What do you think about government invading privacy versus hackers doing so? What about hackers fighting against privacy invasion by hacking?
- If hacktivists didn't exist, would governments be held accountable?

Hacktivists and others

- What are companies' rights versus hackers' rights versus the public's rights?
- What makes you feel safe when connected to the Internet? (Can use arguments from the government and companies, from hackers, or a mix of both. Hackers and government officials do often agree on basic security practices.)
  - What's the difference between security and privacy?

Hacktivists and whistleblowers or hacktivists as whistleblowers

- Are all hacktivists whistleblowers? When do they cross a line?
- Are hacktivist whistleblowers a danger to governments and thus indirectly to people?
- How do they protect the people on behalf of whom they are blowing the whistle?

"Hacking is an illegal criminal activity whereby criminals use a computer to gain unauthorized access to data in a system. Whistleblowing is a legal activity that constitutes exposing any kind of information or activity that is deemed illegal, unethical or constitutes a risk to individuals or the general public. However, if the whistleblowers are hacking in order to expose the illegal or unethical activity, does it make the act of hacking more acceptable to our society as it rides on the back of "the greater good"?...A case of legal double standards?" *From "The Very Fine Line between Hacking and Whistleblowing," Elad Ben-Meir, 2016*

- Can mention "Robin Hood" comparison and applicability

Whistleblowing vocabulary: informant, credibility, undermine, testify

What are some synonyms for whistleblower? Which of these have positive meanings? Which have negative meanings and what are those meanings? In what contexts might you use them?

*Suggested by **Elli Hoffman,** American Assistant*