2023-2024 Middle School Ethics Bowl Case Set

To learn more about this event, please visit:

https://www.ethicsatkentplace.org/student-programs/middle-school-ethics-bowl

Cases Written by the Writing Committee:

Aaden Ray (student), Addie Kostin (student), Ayushi Wadhwa (student), Claire Cherill (student), Erik Kenyon (committee member), Katie MacKay (student), Matt Ferguson (committee member), Mike Britt (teacher), Nicholas Machado (teacher), Oliver Walker (student), Sally Zeiner (teacher), and Sonia Nikhil (student)

And edited for final approval by the Middle School Ethics Bowl Executive Committee:

Ariel Sykes, Deric Barber, Dustin Webster, Erik Kenyon, Karen Rezach, Matt Ferguson, and Roberta Israeloff

Case 2: Zero Days

Bob is the head of a cybersurveillance team at the National Security Administration. His team has been monitoring a group of political radicals, all U.S. citizens, who may be planning a terrorist attack on a domestic target. Bob has many tools at his disposal, one of the most useful of which is a "Zero Day" exploit. What this means is that Bob's team has found accidental flaws in the coding that underlies a social media platform. These coding flaws leave confidential data exposed to be read, altered or even deleted. So far, this has proved a tremendous resource. Bob's team can read the messages which the radicals think are confidential. Members of Bob's team are also able to access credit card records stored in the platform's in-app store. Initial findings indicate that the radical group is using the platform to move funds, possibly in service of a terrorist attack.

Once government agencies discover these coding flaws during a surveillance, they could inform the platform so that the coding errors can be fixed. However, surveillance agencies are not required by law to do this and often don't. Instead, the agencies leave the flaws in place so that agents can extract all the information they can - in this case, about the radicals' plans.

However, the longer the Zero Day exploit continues, the more likely it is that "Black Hat" hackers (hackers with malicious intent) will also discover it and exploit it for their own ends. If this happens, the personal data and credit card numbers of the millions of users of the flawed platform will continue to be exposed - for as long as the government needs to keep the Zero Day exploit going. Unfortunately, there is no way to know how many Black Hat hackers - or anyone else - may also be exploiting this Zero Day.

Some members of Bob's team want to warn the platform's owners immediately to avoid a massive consumer security breach. Others, however, want to stay quiet and continue exploiting the Zero Day. At present, the team does not yet have enough information to determine the nature or scale of a possible terror attack. But the longer the Zero Day exists, the more precise information they can gather. Bob has to make a decision. He feels in a bind with too little information at his fingertips to make the best choice.

Match Question: Should Bob inform the social media platform of the Zero Day now or wait?

Study Questions

1. How far does one's right to privacy extend on computer platforms such as Facebook?
2. When can individuals' rights be violated for the sake of the public good?
3. Does it matter morally that the government does not create Zero Days but merely uses them?
4. Can not doing something count as an action with moral worth?
5. Does the government, in this scenario, have different moral obligations than private individuals or companies?