Case 7b. Social Networks Try to Monitor Their Environments

Synopsis: Case #7b invites you to apply the environmental monitoring framework of Module 7 to judge how social networks should respond to the NGOs and government agencies who are challenging it on issues related to "cyber bullying."

(you must do 7ab-1,7b-2 and 7b-3 if you choose case 7b. Note there are word limits for some questions, but no overall word limit)

Case #7-1. Facebook's Policy on Cyber Bullying

Facebook, the online social networking service founded in February 2004 by Mark Zuckerberg, allows anyone who claims to be at least 13 years old to become a registered user of the website. In 2013 Facebook reported 1.11 billion monthly active users globally. In the Czech Republic Facebook has about 4 million users.

Unfortunately, after Facebook's expansion a serious problem appeared—"cyber bullying." "Cyber bullying" is defined as a young person tormenting, threatening, harassing, or embarrassing another young person using the Internet or other technologies, like cell phones.

Surveys indicate that nearly 43 % of kids have been bullied online. 70 % of students report seeing frequent bullying online. Some 87 % of teenagers who reported cyber abuse said they were targeted on Facebook. Only 37 per cent of those who had experienced trolling ever reported it to the social network where it took place, a UK report found. In the Czech Republic studies show that about 35 % of children have experience with cyber bullying, mostly on Facebook. Emma-Jane Cross, CEO and founder of the NGO **BeatBullying**, notes that many young people suffer in silence when subjected to cyber bullying. **Media psychologist Arthur Cassidy** said online bullying could have a 'massive impact' on older male teenagers. Suicide rates are particularly high amongst this demographic, so it's worrying to hear that teenagers on the whole are choosing to deal with internet abuse themselves, rather than speaking to parents or teachers for help, he said.

Czech legislation includes several laws affecting bullying, including Act. NO 140/1961 Coll., Criminal law: § 231 offense restriction of personal freedom, § 235 offense extortion or § 237

offense oppression. Despite these laws, Facebook bullying hardly gets to the police. One problem is the undefined border between bullying and pranks.

Facebook does not tolerate bullying and says it will remove bullying content when it becomes aware of it and may disable the account of anyone who bullies or attacks another, according to company spokesman Matt Steinfeld.

Facebook has created an online resource centre with suggestions for teens, parents and educators on how to address bullying — both online and off — and take action on Facebook. The site is also beginning to roll out more options for teens to report when posts are making them uncomfortable. The idea is to build on Facebook's existing tools, says Matt Steinfeld. For example, the site unveiled social reporting in 2011, which encouraged users to send a message to a friend asking for help or ask another user to take down a photo. The latter was particularly successful, Steinfeld says: 83 percent of the time, if you reach out to a user who has a photo you don't want to be in, that user will take it off. And Facebook hopes this will be true of bullying as well. The hub gives suggested conversation starters for victims ("Hey, NAME — that comment wasn't funny. I don't like it, please take it down"), as well as for people who are accused of bullying and people who witness it. Facebook also has added a number of other advisories on its websites:

- If you're not happy with a post you're tagged in, you can remove the tag.
- If you need to escalate the issue, you can *unfriend* or block the person.
- If the post is abusive, please report it to us.
- If you want help, reach out to someone you trust, like a parent or teacher.
- If you see a friend being targeted or bullied on Facebook, please report this to us. If you think your friend needs help right away, let someone you trust know, like a parent or teacher.

Besides the information for children and teens users, Facebook also offers advice for their parents. The most important question for parents is: "How can I help my teen use Facebook wisely?"

Facebook has written: "Depending on your teen's age, you might go through their privacy shortcuts and account settings together and make selections you're both comfortable with. No matter how old your child is, we recommend that you make using Facebook responsibly part of an ongoing conversation about the internet and technology. Talk about your expectations

about how they'll behave and help them understand what's safe and what they need to be aware. Be sure your teen understands these basics of internet safety:

- Never share your password
- Think before you post
- Only accept friend requests from people you know personally
- Report anything that looks suspicious (learn how)

Facebook staff say the company is serious about this issue. "Bullying prevention has been something we've worked on for a long time," Facebook has declared. "We are the first Internet company that's putting bullying prevention resources in the heart of the product itself." On the other hand, bullying on Facebook continues to be a major problem, raising questions as to whether Faceebook's measures are improving safety on the world's largest social websites.

Questions:

1. **(2) Identify two organizations and two internet sites Facebook should be monitoring to make sure it stays ahead of the bullying issue so that the issue does not present major problems for the company. Segregate your answers and be as specific as possible in each category:**
   a. **Organizations**
   b. **Internet sites**

NOTE: "Be as specific as possible in each category" means precisely that. I expect you to name specific issues, organizations, internet sites and print or electronic media! In previous classes, many students tended to give generic answers!

2. (2) Choose 1 "signal" in the Facebook environment that you would categorize as particularly "strong?" If you cannot identify one strong signal, choose a weaker signal and assess its strength. (explain you assessment using the 3 prescribed metrics for measuring the strength of signals—strength, timing, and potential impact.)

(maximum length for Q3 60 words)

This case was prepared by Jitka Novotová, a student at the Technical University of Liberec, under the direction and with the assistance of Professor Earl Molander.

Case #7b-2. Yik Yak Faces Cyberbullying Abuse on Its Website

Yik Yak is a U.S. social media network like Facebook and Twitter only without user profiles or virtual community bulletin boards with the individual poster identified. Other similar on-line sites are **Whisper** and **Secret**.

Yik Yak sorts followers geographically, even by university, not by friends or followers as Facebook and Twitter do. Only posts within a 1.5-mile radius appear. At Apple's App Store,Yik Yak surpassing competitors like Whisper and Secret in popularity. At times, it has been one of the store's 10 most downloaded free phone apps.

Yik Yak was created in late 2013 by Tyler Droll and Brooks Buffington. With Yik Yak, their goal was to create a more democratic social media network, one where users didn't need a large number of followers or friends to have their posts read widely.

Mr. Droll and Mr. Buffington started Yik Yak with a loan from Mr. Droll's parents. (His parents also came up with the company's name, which was inspired by the 1958 song, "Yakety Yak.") In November 2014, Yik Yak closed a $62 million round of financing led by one of Silicon Valley's biggest venture capital firms, Sequoia Capital, valuing the company at hundreds of millions of dollars.

On its home page YikYak describes itself as "a social app that lets people discover their local community. The app instantly connects people to everyone around them so they can share news, crack jokes, offer support, ask questions, and interact freely. Yik Yak is home to the casual, relatable, heartfelt, and silly things that connect people with their community."

Yik Yak is organized into "communities" of common interest, with a moderator managing each community, deleting what they consider inappropriate posts.

However, **Yik Yak** also has become a popular social resource for college students across the U.S. to find a party, commiserate about final exams or professors who gave them a bad grade, or slander a fellow classmate. "Yik Yak is the Wild West of anonymous social apps," said Danielle Keats Citron, a law professor at University of Maryland and the author of "Hate Crimes in Cyberspace." "It is being increasingly used by young people in a really intimidating and destructive way."

Colleges are almost powerless to deal with Yik Yak. The app's privacy policy prevents schools from identifying users without a subpoena, court order or search warrant, or an emergency request from a law-enforcement official with a compelling claim of imminent harm. Schools can block access to Yik Yak on their Wi-Fi networks, but banning a popular social media network is controversial, tantamount to curtailing freedom of speech. And students can still use the app on their phones with their cell service.

Last fall, an incident at Eastern Michigan University highlighted the problem with Yik Yak. The professors were lecturing about post-apocalyptic culture, some of the 230 or so freshmen in the auditorium had been having a separate conversation about them on a social media site called Yik Yak. There were dozens of posts, most demeaning, many using crude, sexually explicit language and imagery.

After class, one of the professors, Margaret Crouch, sent screenshots of some of the worst messages to various university officials, urging them to take some sort of action. "I have been defamed, my reputation besmirched. I have been sexually harassed and verbally abused," she

wrote to her union representative. “I am about ready to hire a lawyer.” Because Yik Yak is anonymous, there was no way for the school to know who was responsible for the posts.

Since the app was introduced a little more than a year ago, it has been used to issue threats of mass violence on more than a dozen college campuses. Racist, homophobic and misogynist “yaks” have generated controversy at many more. At one school, a “yakker” proposed a gang rape at the school’s women’s center.

Because the Yik Yak app is free, like many tech start-ups, it doesn’t generate any revenue. Attracting advertisers could pose a challenge, given the nature of some of the app’s content. For now, though, Yik Yak is focused on extending its reach by expanding overseas and moving beyond the college market, much as Facebook did.

Yik Yak has made some changes to their product, e.g., adding filters to prevent full names from being posted. Certain keywords, like “Jewish,” or “bomb,” prompt this message: “Pump the brakes, this yak may contain threatening language. Now it’s probably nothing and you’re probably an awesome person but just know that Yik Yak and law enforcement take threats seriously. So you tell us, is this yak cool to post?”

In cases involving threats of mass violence, Yik Yak has cooperated with law enforcement authorities. In November 2014, local police traced the source of a “yak” — “I’m gonna [gun emoji] the school at 12:15 p.m. today” — to a student’s dormitory room. The student was arrested within two hours and pleaded guilty to making a false report or terrorist threat.

In the absence of a specific, actionable threat, Yik Yak protects the identities of its users. The responsibility lies with the app’s local “communities” to police themselves by “upvoting” or “downvoting” posts. If a yak receives a score of negative 5, it is removed. “Really, what it comes down to is that we try to empower the communities as much as we can,” Mr. Droll said.

Yik Yak says it has built virtual fences — or “geo-fences” — around about 90 percent of the nation’s high schools and middle schools because of the widespread abuses when the app was first adopted by young students. “We made the app for college kids, but we quickly realized it was getting into the hands of high schoolers, and high schoolers were not mature enough to use it,” Mr. Droll said. These fences actually make it impossible to open the app on school grounds. Yik Yak also changed its age rating in the App Store from 12 and over to 17 and over.

Parental advocates are skeptical. Ob Zidar, co-founder of **Third Parent,** a company that audits teen use of social media, argues that if Yik Yak was doing its job, there would be far fewer incidents of its misuse and abuse.

Yik Yak’s Demise

In mid-April 2017, Yik Yak co-founders Tyler Droll and Brooks Buffington published a farewell note to users, announcing they would shut down their once-popular anonymous social network this week. During its 4-year short life, Yik Yak had raised $73.4 million in venture, with a valuation approaching $400 million in 2014, its halcyon days.
The app was plagued by cyberbullies of every kind and even banned by some schools. In 2015, Yik Yak had to admit to users that they were only masked from each other, not police

officers or other authorities with a warrant. And then in 2016, security researchers with New York University found other ways to hack users' personally identifiable information out of Yik Yak. All the while, cyberbullies and unsavory content drove down the app experience for others. By the end of 2016, user downloads had declined 76 percent versus the same period in 2015, and the company began laying off most of its employees.
Yik Yak is not the first anonymous chat app to hit the "deadpool." Secret also went out of business in 2015. And the company won't be leaving a hole in the market, exactly.
Yik Yak competitors still in business include: **Whisper**, the anonymous chat and sharing app; Kik, which only requires usernames; Blind, the anonymous workplace chat app where Uber employees have recently aired grievances; and 7 Cups, where people can go for "active, non-judgmental listeners."

Appendix 1: What Account Information Does Yik Yak Have?

Yik Yak records a user's IP address at the time of the app's installation. In addition, Yik Yak maintains a log of the following information for each message posted:

- The IP address from which the message was posted;
- The GPS coordinates of the location from which the message was posted;
- The time and date when the message was posted; and
- The user-agent string associated with the device from which the message was posted

Yik Yak will also require its users to provide a phone number when posting content to the app or if Yik Yak suspects improper activity.

Appendix 2. Data Retention and Preservation Requests

Yik Yak retains different types of information for different time periods. Due to the real-time nature of Yik Yak, some information may be stored for only a very brief period of time.

Yik Yak will not retain data for law enforcement unless it receives a valid preservation request. Preservation requests must be submitted in writing, on official law enforcement letterhead, and signed by the requesting official. Please include screenshots of the messages that you wish to be preserved, if available. Requests may be sent as an email attachment (our contact information is below).

Appendix 3. Legal Process Requirements

Yik Yak discloses user account information only in accordance with applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq. Yik Yak will only release non-public information about its users to law enforcement officials in response to appropriate legal process, such as a subpoena, court order, or search warrant – or in response to a valid emergency request, as described below. Under the SCA:

- A valid administrative, grand jury, or trial subpoena in connection with an official criminal investigation or prosecution is required to compel Yik Yak to disclose certain specific types of "basic subscriber information" (defined in 18 U.S.C. § 2703(c)(2)). Yik Yak's records of "basic subscriber information," that can

be disclosed in response to an appropriate subpoena will generally be limited to (1) the telephone number provided by the user, (2) the user's IP address at the time of installation, and (3) the time and date when the user installed the app.

- A court order issued under 18 U.S.C. § 2703(d) is required to compel Yik Yak to disclose certain non-content records associated with a user's account. This could include (1) the time and date when a message was posted, (2) the IP address associated with a specific message, (3) the GPS location from which the message was posted, and (4) the user-agent string associated with the device from which the message was posted.
- A search warrant is required to compel Yik Yak to disclose the contents of any messages associated with a user's account. In addition, the SCA permits Yik Yak to disclose the non-content records described above in response to a search warrant.

Any legal process submitted to Yik Yak should include a detailed description of the specific Yik Yak post(s) that you are seeking information about, including the exact language of the post, and if known, the approximate time, date, and location of the post. Please provide screenshots of the posts if available.

Appendix 4. Emergency Requests

Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), Yik Yak may disclose user account information to law enforcement – without a subpoena, court order, or search warrant – in response to a valid emergency when we believe that doing so is necessary to prevent death or serious physical harm to someone (for instance, in cases involving kidnapping, bomb threats, school shootings, or suicide threats). Yik Yak evaluates emergency requests on a case-by-case basis.

Any information Yik Yak provides in response to emergency requests is limited to what we believe would prevent the harm. This may include a user's IP address, GPS coordinates, message timestamps, telephone number, user-agent string, and/or the contents of other messages from the user's posting history.

Law enforcement officers can submit an emergency request as an email attachment (our contact information is below). Emergency requests must be submitted on law enforcement letterhead, and must include the following:

- a detailed description of the emergency;
- a description of the harm to be prevented;
- a detailed description of the Yik Yak post that you are seeking information about, including screenshots, if available;
- the specific information requested, including an explanation of why that information is necessary to prevent the harm;
- an explanation of why the information is needed without waiting for legal process
- and the signature of the submitting law enforcement officer

Please note that Yik Yak cannot review or respond to emergency requests sent by non-law enforcement officials. If you are aware of an emergency situation, you should immediately contact your local law enforcement officials.

Source: www.yikyak.com website

Questions:

3.(2) Explain YikYak's demise as a failure to correctly read environmental signals?

(maximum length for Q6 100 words)

Case 7b-3. Whisper Survives as an Anonymous Chat Site

Have you ever heard of the app, "**Whisper"**? It has been described as "the place to go these days to vent, come clean, or peer into other people's secrets," and that the goal is that of "turning confessions into content."

Whisper is a mobile app available without charge, which claims to allow users to post and share photo and video messages anonymously, although this claim has been challenged with privacy concerns over Whisper's handling of user data. The postings, called "*whispers*," consist of text superimposed over an image, and the background imagery is either automatically retrieved from Whisper's own search engine or uploaded by the user. Whisper was co-founded in March 2012, by CEO Michael Heyward, the son of the entertainment executive Andy Heyward, and Brad Brooks, who is the CEO of mobile messaging service TigerText. As of March 2017, Whisper has a total of 17 billion monthly "pageviews" on its mobile and desktop websites, social channels and publisher network, with 250 million users monthly (up from 20 million in 2015) across 187 countries.

Anyone can post an anonymous message to Whisper. When you open the app, you see six such images. Each one has a "secret" on it. You can respond to a message publicly or privately, choosing a public anonymous post or a private pseudonymous chat. Users don't have a public identity in the app. While they do have "handles," there's no way to contact them except through the messages they post.

In terms of demographics, The New York Times named Whisper in September 2015 as a social media platform of choice for Generation Z (Generation Z starts with the birth year 1993) in an article about Internet habits among Generation Z and Millennials (the generation that starts with birth in the early 1980s, ending in the mid-1990s). As of June 2017, 75% of Whisper's users were between the ages of 18 and 34, and predominantly female. Whisper's Facebook page was the top-performing media fan page for interactions on the social network with approximately 200 million interactions in fiscal year 2016

The Whisper Concept and Anonymity

Whisper purports to promote online anonymity and claims this will prevent and combat cyberbullying. In October 2015, Whisper announced a partnership with the Ad Council on the "I Am A Witness" anti-bullying campaign, along with other tech companies, including Facebook, Twitter, and Snapchat. In March 2016, Whisper announced a partnership with the Anti-Defamation League's Best Practices for Responding to Online Hate.

Whisper's anonymity is claimed to have fostered a support network where concern and care among users has developed. Another premise behind the service was to counter the "best possible self" ego-driven self-aggrandizing "vanity" posting done on Facebook, and as an antidote to the phenomenon of "oversharing" and "too much information" that young users engage in online.

The U.S. business magazine Forbes, and others have called Whisper "the anti-Facebook," One digital-news website summed up all these points together: "In addition to preventing cyber bullies, Whisper gives users the opportunity to confess to things that could potentially ruin marriages, friendships or result in loss of job, without suffering consequences. You can over share without any repercussions." Another news source described Whisper as "…a new type of social sharing, the kind that won't come back to haunt you."

Controversy over Whisper's Privacy Policy

The Whisper app has been criticized for requiring access to smartphone features such as the camera and the user's contact list, which is disclosed when the app is downloaded on the Android

The company's privacy policy reveals that it will turn over information in the case of requests from law enforcement in order to comply with applicable laws for enforceable government requests such as a subpoena. The Electronic Frontier Foundation's attorney Hanni Fakhoury commented in early 2014 that while Whisper may have no legal choice in the matter, "it's the doublespeak that's problematic." Fakhoury elaborated that: "You have to be very careful about selling a program as a secure way to secretly communicate, and then reserve the right to turn over that information whenever necessary."

The Guardian Allegations

In October 2014, the British newspaper The Guardian newspaper alleged that:

- Whisper retains every user's posts indefinitely in a central database (including "deleted" posts), together with each post's timestamp and approximate geolocation, even if the user has opted out of geolocation;
- Whisper allegedly stores or processes user information outside the United States despite having told its users that "we process and store all information in the United States". Whisper has said that while it does use an outsourcing firm for content moderation based in the Philippines, no data is stored outside the US.
- Whisper allegedly provides data it gathers (including geolocation data) to the FBI, and MI5. Whisper participated in a DOD project about suicide prevention by sharing aggregate mentions of certain words on military bases.

Whisper disputed nearly all the Guardian allegations and made a point-by-point response to the Guardian. After reading Whisper's response, Twitter's former security head Moxie Marlinspike commented on Hacker News that Whisper "should never have claimed to provide anonymity if it had to track users to make the app function". He pointed out that there are many "hard problems" that need to be solved before a service can claim to provide truly unlinkable anonymity, and that "there are projects like Tor that are approaching these types of problems seriously, but apps like Whisper or Secret end up poisoning the well and confusing users".

In March 2015, The Guardian published a clarification of the October 2014 piece in which it had made numerous allegations about Whisper's privacy protection and metadata policy. The Guardian clarified the claims regarding user location, data storage, changes to Whisper's terms of service and security policy and the sharing of user data with the US Department of Defense. It also removed an opinion piece titled "Think you can Whisper privately? Think again."

Xipiter report

On March 22, 2015, a security startup called Xipiter published a report in which they outlined serious security concerns and the resistance they met when trying to bring these concerns to the attention of Whisper. Xipiter claimed that it could hijack a users' account, post (publicly or privately) as a hijacked user, and view all of a user's current and past private messages. In response, Whisper claimed that it is not possible to do such things with their app and accused Xipiter of fabricating their proof of concept video. Xipiter's claims have yet to be validated or disproved by independent security researchers.

4. Choose one "signal" in the Whisper environment that you would categorize as particularly "strong?" If you cannot identify a strong signal, choose a weaker signal and assess its strength. (explain your assessment using the 3 prescribed metrics for measuring the strength of signals—strength, timing, and potential impact.)

(maximum length for Q4 60 words)