

Case #7b. Yik Yak Confronts 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.

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:

1. Having critiqued Facebook's policy regarding protection against the use of Facebook as a vehicle/channel for bullying, how would your answer differ regarding YikYak?
2. What issues, organizations, internet sites and media should Yik Yak be monitoring that would be different from those of Facebook to make sure it stays ahead of this issue and the issue does not present major problems for the company. Segregate your answers and be as specific as possible in each category:
 - a. Issues
 - b. Organizations
 - c. Other Internet sites
 - d. Media
 - e. Other?