Privacy
Fall 2016
Prof. Ford

Take-Home Final Exam

This take-home final exam is worth 60% of your course grade. It will be administered on Thursday, December 15, 2016. You have eight hours to complete the exam (or twelve hours if you have been granted an accommodation by the Registrar's Office). At the conclusion of the exam, responses must be emailed to the Registrar's Office at **registrar@law.unh.edu**.

Please do not put your name or any identifying information on your exam. Place only your assigned exam number on the top right corner of your answers.

Please format your responses similarly to this document: **single-spaced, with 1.5-inch margins, and empty space between paragraphs**. Use 12-point Cambria, Century, Constantia, or Book Antiqua; do *not* use Times New Roman. Number your pages. I recommend you submit your answers as a PDF file.

You may consult **any existing material you wish** while completing this exam. **You must write your entire response, yourself, during the exam period; you may not paste any previously written material into your answers**, whether written by you or anyone else. **You may not discuss the exam with anyone while it is being administered,** including other students, attorneys, or participants on online discussion boards. Please type the following at the top of your exam:

> I affirm that I have not discussed this exam with other students or anyone else during its administration.

This exam consists of **four questions, of which you should answer any three.** (Scenario A contains two questions; scenarios B and C contain one each.) **There is a total word limit of 4,000 words for your entire exam.** There is no need to include the questions in your responses. **Please list your word count at the end of your exam.**

If any of the questions are unclear, or don't provide necessary information, state explicitly any assumptions you make and explain how your answer depends on those assumptions.

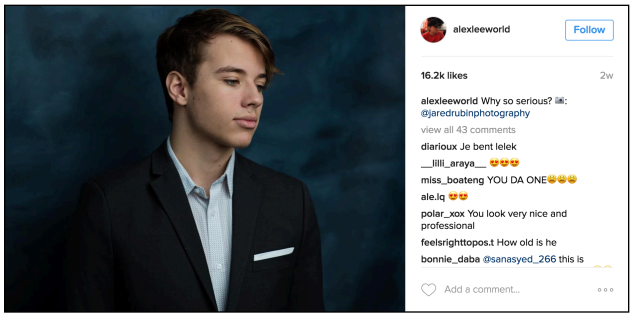
Good luck and have a wonderful winter break!

Scenario A

Remember Alex from Target? In 2014, Alex Lee was a 16-year-old student and part-time Target cashier in Frisco, Texas. Then someone with the Twitter handle @auscalum tweeted a surreptitious photo of him (shown at right) and #alexfromtarget became an overnight internet sensation. (Turns out @auscalum didn't take the photo; someone with the handle @brooklynjreiff took it and tweeted it, and @auscalum later found it on Tumblr. It didn't go viral till @auscalum's tweet, though.)

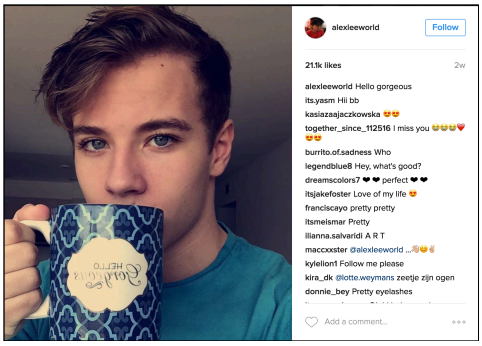
Over the course of a single eight-hour shift, Alex went from 114 Twitter followers to 100,000; within two weeks he had 730,000 on Twitter and 2.3 million on Instagram. Within a few days he made an appearance on *Ellen;* he turned down many other invitations. The *New York Times* described what happened next:

> [Two weeks later] Alex says he can barely go outside for fear of being accosted. "I've been in the house the entire time," he said. "I'm kind of scared to go in public."
>
> When he walked into school last Friday, his first day back since becoming #alexfromtarget, students stopped him every few feet to snap selfies. In speech class, he sat with classmates and watched his appearance on "Ellen." And after school, when Alex went to Whataburger with his father, he opened the door and was met with squeals of "Allllleeeeeexxxx!!" and was chased out by cellphone-toting screaming teenage girls.
>
> While Alex is clearly enjoying some of the attention, he and his family have also had to deal with more serious consequences of web fame. A crafty marketing firm, Breakr, tried to take credit for Alex's rise. (Everyone the company claims it worked with, including Alex's family and @auscalum, has denied ever hearing of Breakr. In a report, BuzzFeed said that the company's claims simply don't add up.)
>
> Thousands have taken to social media to call Alex names (including vulgarities) or fabricate stories about him being fired. Twitter is littered with posts that denigrate his looks (e.g., "Alex from Target is so damn ugly") or spew envy at him ("Alex from Target is a nobody who doesn't deserve fame").



There have even been dozens of death threats on social media and in private messages ("Alex from target, I'll find you and I will kill you").

Alex is no stranger to some of this behavior. He told me he was bullied in elementary school and has learned to disregard "the hate" — though, he said, it's increasingly difficult to ignore. But his parents, who are incredibly happy for Alex, say this hostility has been difficult to watch.



"The biggest concern for myself and my wife is some of the negativity we're seeing online," said his father, Eric Fooks, who is a small-business consultant. "Our concern is making sure he's safe."

Mr. Fooks said that in addition to death threats, people have leaked the family's personal information online, including Social Security numbers, bank accounts and phone records. The family, worried for the safety of Alex and his five siblings, has been in contact with the local police. Alex's parents have met with his school's principal and security officers, as well as Target managers, to put together security plans in case of an emergency.

Two years after his photo went viral, the kid the *Times* described as "shy and exceedingly polite" seems to be making a go of it as a model/actor and professional social influencer. (A few of his recent posts are shown above.) Today, he has 1.7 million followers on Instagram and 2.3 million on Facebook (in all cases @AlexLeeWorld); on those profiles he prominently lists an email address for sponsorship inquiries. A recent *Bloomberg Businessweek* piece on social influencers reported that someone with Alex's following can expect to get $10,000 per sponsored post. (Great piece; highly recommended, though probably not till after the exam is over.)

Question 1: Does Alex have any meritorious legal claims against anyone for invasion of his privacy? Explain.

Question 2: Whether or not Alex has any legal recourse, should he? Against whom? Explain, drawing on the various privacy interests, theories, and policies we have discussed throughout the course. Be sure to discuss counterarguments.

Scenario B

One trend in employment law concerns companies that ask their employees to use wearable devices like Fitbits or Apple Watches that track step counts, pulse rates, and so forth. Companies like it when employees do this because the employees tend to become more active, and so healthier, lowering the companies' health-insurance costs. Some companies and health insurers have even provided the devices for free or at a significant discount through what are known as wellness programs. These programs have become popular: one survey found that 31% of companies with 1,000 or more employees offered wearable activity trackers to employees, with another 23% considering whether to do so in the next two years. At TransUnion, the credit bureau, more than 1,000 employees wore Fitbits as part of a wellness contest. Winning employees won prizes and the winning office got to direct a charitable contribution.

Fitbit has been a leader in wellness programs. It offers bulk discounts on devices and makes a corporate app that it offers to companies that buy the devices. Fitbit's app can be set up to share employees' exercise and sleep patterns with the employer. This lets a company set up challenges between teams or reward employees who meet activity goals. At most companies, the programs are optional, with participating employees getting anything from a discounted or free device to discounted insurance premiums. A few companies, however, have started to experiment with mandatory programs.

One particular industry where the use of wearable devices has expanded in recent years is professional sports. Many teams equip their players with devices that measure movement, heart rate, respiration, and so forth during practices — far more information than is provided by a Fitbit. (This hasn't happened yet during games, as far as I know, though the day may be coming.) These devices gather data that lets teams measure how much effort players are exerting, helping them monitor health and conditioning and figure out how to optimize their lineups for games. Use of these devices is typically mandatory, though players unions have started to consider whether to object.

Question 3: What are the privacy implications of companies providing wearable devices to employees? What are the privacy risks and how should companies guard against those risks without sacrificing the utility of wearable devices? Are the privacy implications different for ordinary office employees as compared with, say, professional basketball players? Explain, drawing on the various privacy interests, theories, and policies we have discussed throughout the course.

Scenario C

An IMSI catcher, often called a cell-site simulator or a stingray, is an electronic surveillance device often used by military, intelligence, and police officials. (One model is shown at the right. Typically one is mounted in a truck, which provides power, an antenna, mobility, and so forth.) The device broadcasts a signal pretending to be a cell tower; when cellphones try to respond and connect to the tower, the stingray records their international mobile subscriber identity numbers (which are unique ID numbers identifying particular phones) along with information like the date and time. Stingrays let authorities determine which phones are located near a given location at a particular time. They can also record information provided by those phones, such as the phone numbers a phone tries to call while connected to the stingray. They don't get access to call content, though.

Much of the information stingrays provide is available through other means. For instance, cellular network providers keep logs of which phones connect to which cell towers; police can obtain these logs after the fact. Police have used this capability to identify suspects. If, for example, the same cellphone connected to towers near five banks around the times each was robbed, then the phone's owner should probably be investigated. Stingrays let police obtain similar info without going through network operators, who may demand a warrant or court order. So if a police agency wants to record the phone number of everyone located near a protest, for instance, it can just deploy a stingray and gather that information itself. Indeed, police have deployed stingrays near various protests, including the Occupy Wall Street protests and the pipeline protests at the Standing Rock Sioux Nation in North Dakota.

Melody Dalquist is a Standing Rock protester, one of a core group of about 40 who have spent months at a camp near the site of the proposed oil pipeline. One day, while driving on a public highway from the camp to a nearby town to purchase supplies, she was directed through an FBI checkpoint. At the checkpoint each car was told to stop for about 15 seconds, after which most drivers were told they could proceed. Dalquist, though, was directed to the side, where she was arrested for her role in the protests.

Dalquist's lawyer learned during discovery that the FBI had deployed a stingray early on in the protests, which agents used to compile a list of phones they suspected of belonging to protest leaders. The FBI did not obtain a warrant or

court order before deploying the device. When Dalquist drove through the checkpoint, her car was scanned from the outside with another stingray, which picked up a signal matching the list of suspect phones. When she was arrested, her phone was seized and police confirmed that it matched one located near the protest camp.

Dalquist's lawyer files a motion to suppress the stingray evidence and arrest, arguing that the information came from a warrantless search performed in violation of the Fourth Amendment, as applied to the states through the due-process clause of the Fourteenth Amendment.

Question 4: You are a law clerk to Judge Quinn of the United States District Court for the District of North Dakota, to whom the Dalquist case has been assigned. Judge Quinn tells you that she cannot find any case law directly on point. She asks you how she should rule on the motion to suppress based on the Supreme Court's cases applying the Fourth Amendment in related contexts and based on the underlying policy considerations discussed in those cases. Answer her question in a short memo.