Case Study #2: Kant & the Ashley Madison Hack

Read the section on Kant in our text and the attached article from *The Verge*, and then answer the following questions. **The completed assignment should be two pages long, (approximately 1400 words) using 12 pt. fonts and single spacing with one inch margins. Please follow the assigned format as exemplified at the end of your first case study assignment. Each answer should be separated, numbered and proportionate to the number of points possible. This study is worth a total of 60 points.**

*Your completed assignment is due on the 11th of November.*

*Please refer to the first assignment for general suggestions, grading rubrics, and a sample completed assignment!*

1. **Extract and paraphrase** Casey Newton’s argument in the attached article from *The Verge* concluding that we ought to hold companies responsible when they fail to protect our data. (5 points)

2. **Asking the right questions:** What facts would you need to know about this case to make a reasonably informed judgment? In this section, note that you should be raising questions such as the frequency and breadth of such hacks, the agreements between companies and the users of their sites regarding data security, the number of users who were married at the time of accessing Ashley Madison’s services, etc., but not questions about Kant. **Provide as a bulleted list and pose in question form.** For this assignment, you do not have to do all the research but you need to raise the kind of questions that would drive such a project. These should be research questions and as such should be concrete and answerable. No bias or prejudice should be evident and the questions should be non-normative (no “ought” or “should” questions). Think about facts that, if known might help determine how one should or could respond to the case. (15 points)

3. **Kant’s Position:** Pending the acquisition of all of this information, how do you think Kant would respond to this case? Who is really most at fault here – the company for not adequately protecting the data, the hackers who released the data or those website users who were looking for adulterous affairs? Be sure to provide citations from Kant (*primary source = Kant’s writings and does not include secondary commentary from Rosenstand or from me*) to support your answer. In citing the quote, all you need do is indicate the page from the text (see example). Note that this question carries the highest weight in points. (25 points)

4. **Critical Objection:** Identify one key problem with Kant’s deontic approach ethics as it applies to this particular case. (10 points)

5. **Conclusion:** Who do you think is most at fault here – the company for not adequately protecting the data, the hackers who released the data or those website users who were looking for adulterous affairs? Defend your answer without resorting to a repetition of points made in previous sections. (5 points)
Background\(^1\): Case Study #2

The Verge

The mind-bending messiness of the Ashley Madison data dump\(^2\)

Casey Newton

August 19, 2015

Massive data breaches have become so routine as to become background noise. In the past year, half of American adults had their personal information exposed as a result of hacks, the *New York Times* reported. And yet while every hack produces anguished headlines and hand-wringing, the impact of the data breaches on average people is small. Hackers may gain access to your email address, or your phone number, or an encrypted password. But any financial losses are typically absorbed by your bank. We glance at the headlines, change our passwords, and await the next minor inconvenience.

The *apparent release last night* of personal information for 32 million registered users of AshleyMadison.com, a website for connecting people who want to have affairs, is likely to have much more profound consequences. Impact Team, the group of anonymous hackers who are taking credit for the breach, sought to have Ashley Madison's website taken down *in protest of the company's business practices* and its encouragement of adultery. But the practical impact of the breach is likely to be much broader. There are a lot of threads here, and it's worth sorting them out.

*The consequences for Ashley Madison are likely to be catastrophic*

---

\(^1\) Please note that you are not limited to the background offered. It is expected that you will do a bit more in-depth reading to develop your thesis. You may feel free to use any credible/reliable source as evidence for your arguments. Additionally you may use additional material from Aristotle to defend your answers. Please provide full citation for all research.

The consequences for Ashley Madison are likely to be catastrophic. A CEO who routinely bragged about the company’s privacy features now seems likely to face a barrage of lawsuits from members who have found their information exposed. And a site that depends on privacy and security to earn members’ trust may find it impossible to win it back.

The legal consequences are likely to extend beyond lawsuits. As the Washington Post noted, adultery is a crime in the military, and thousands of Ashley Madison users had email addresses from the .mil domain. It’s impossible to say how many of the addresses are valid — Ashley Madison did not require users to verify their email addresses.

But under military rules, servicemembers found guilty of philandering can be punished by a year of confinement. They’re also subject to a dishonorable discharge, which would mean losing their pension.

For registered members of the site, the personal consequences could be dire. The data dump has already been turned into a searchable database, and the search results will be devastating. For some, it will confirm suspicions; for others who decide to check it on a lark, it may raise awful new questions. And that’s true even though simply being registered for Ashley Madison tells you very little about a person. People have all sorts of arrangements in their relationships, and odds are they don’t share that information with their friends and family. Put another way: plenty of people were using Ashley Madison with their partners’ consent.

It’s likely that millions more people who registered for Ashley Madison never consummated an affair — among other things, the ratio of men to women on the site was roughly 6 to 1, according to an analysis of the Impact Team data. That said, millions of people likely used the site to seek partners outside their relationships. The cheaters will despair; relationships will end; children’s lives could be affected for the worse.

**People could lose their jobs as a result**

And the pain won’t end there — certain employers will react negatively to the knowledge that their employees were used the site, and people could lose their jobs as a result.
Government employees who could become subject to blackmail; schoolteachers in more conservative districts; elected officials; CEOs — all of these could face professional consequences, along with anyone else who has a morals clause in their employment contract. And the results could follow them — expect this data to become included as a part of pre-employment background checks for years to come.

© Provided by The Verge

For those who never signed up for Ashley Madison, or had a partner who did, ethical questions will still come fast and furious. As John Herrman notes at The Awl, many of us will feel tempted to see which of our friends, family members, and coworkers may have registered for the site. When Target was hacked, few would have cared if it resulted in their purchase history being made searchable. Looking through the Ashley Madison data will be at least as tempting as looking through the leaked nude celebrity photos of last fall’s Celebgate hack. Only this time you’ll likely be looking not for a celebrity, but for someone you know. And what if you find something? How will you react? How will the person you’re snooping on? At various times, all of us are terrible in our own ways. What happens when those ways are easily searched on a public database?

What if you find something? How will you react?

The worst impact of the Ashley Madison breach will surely be personal: while incredibly common, cheating also upends people’s lives and can lead to personal and professional ruin. Hopefully it leads companies to adopt better privacy and security practices — Ashley Madison, for all its boasting, made several crucial errors in attempting to keep members’ information anonymous.

But if we’ve learned anything from the never-ending series of data breaches, it’s that over a long enough time period, all sites are likely to fall victim to hackers. And this raises yet more questions. In a world where we expect more of our communications to eventually be made public, will we begin to abandon certain apps or services en masse? Is it truly our responsibility to act as if everything we say will eventually become public, or can we hold companies responsible when they fail to protect our data? Can we pressure companies to
purge more of our data on a regular basis, limiting our exposure risk in the likelihood of an eventual hack? Or will we once again shrug our shoulders at the seeming hopelessness of it all?

At this early stage, it's impossible to say. And so we sit and stew about a future that could someday come to include a searchable online database of our emails, or our text messages, or our Tinder chats. We can hope that future never comes about, even though it seems to grow closer with every passing hack. In the meantime, two old adages would seem to apply. So prepare for the worst. And mind your own business.