Privacy and Safety Concerns: What Protections Do Online Dating Services Owe Users?

Case

Author: Brendan D. Dooley
Online Pub Date: January 15, 2020 | Original Pub. Date: 2020
Subject: Business Ethics, Risk Management, Information Management
Level: Intermediate | Type: Indirect case | Length: 2777 words
Copyright: © Brendan D. Dooley 2020
Organization: Ashley Madison| OKCupid| Tinder | Organization size: Medium| Large
Region: Northern America | State:
Industry: Information and communication
Originally Published in:
Publisher: SAGE Publications: SAGE Business Cases Originals
DOI: http://dx.doi.org/10.4135/9781529724905 | Online ISBN: 9781529724905
This case was prepared for inclusion in SAGE Business Cases primarily as a basis for classroom discussion or self-study, and is not meant to illustrate either effective or ineffective management styles. Nothing herein shall be deemed to be an endorsement of any kind. This case is for scholarly, educational, or personal use only within your university, and cannot be forwarded outside the university or used for other commercial purposes. 2020 SAGE Publications Ltd. All Rights Reserved.

This content may only be distributed for use within CQ PRESS.
http://dx.doi.org/10.4135/9781529724905
Abstract

In 2015, Ashley Madison, an online dating service of a different sort, was targeted by a hacking group. The “white hat” hackers threatened to release the entirety of their user base should the website fail to meet its demand to close its operation. Under normal circumstances the threat would arouse vigorous sympathy for the targeted company and its customers. The thought of having private, romantic correspondence released online for all to see strikes most as a scandalous threat, one deserving an unrepentant response from criminal justice authorities, the business community, and consumers alike.

However, Ashley Madison is an online dating service catering for a different clientele. Its trademarked corporate slogan is provocative: “Life is short. Have an affair.” For some, this fact changes the moral calculus of how we evaluate the data dump that a secretive group known as the Impact Team provided, as cheaters do not make for sympathetic victims. Others insist that several weighty ethical considerations remain that must be confronted. Using this admittedly dramatic example, the present case study draws links with a couple of core concerns that impact all online dating. First, what protections does a provider owe to its users? Second, what obligations ought to inhere in managing complications arising in real life from activities facilitated through online connections? Both relate to an all-encompassing concern over what, if any, fiduciary obligations online providers should assume when offering their services. Students will be asked about the responsibilities of online dating providers and approaches these providers could use to assure security of sensitive information.

Case

Learning Outcomes

By the end of this case study, students should be able to:

• Provide an argument as to whether the release of the Ashley Madison list of patrons was defensible or not.
• Evaluate where mistakes in managing client information and improvements might be sought.
• Outline how wide or restrictive the scope of responsibility for online dating providers should be.

Introduction

On July 15, 2015, Avid Life Media (ALM) received a threat from a hacking group identifying itself as the Impact Team. Avid Life Media is the parent company of Ashley Madison and Established Men. The former advertises its services under the slogan “Life is short. Have an affair.” The latter company caters for women, attempting to connect them with “successful and generous benefactors to fulfill their lifestyle needs.” The company is therefore openly engaged in a business practice that many find in violation of deeply held moral convictions, profiting in the wake of considerable damage of which spouses, children, and extended family members will bear the brunt. The company shows little embarrassment from bartering in adulterous behavior. Indeed, its attitude only enhances its brand as a renegade.

Like the group of Internet vigilantes dubbed Anonymous, the Impact Team styled itself as a group of saviors serving to chase smut dealing from the likes of ALM from the Web. Applying the same technological know-
how of “black hat” hackers who use their abilities to advance criminal ends, so-called “white hat” groups can work to defend victims against predatory behavior. Much like the example of a serial murderer who kills only child molesters, the use of criminal behavior in the present instance invited the criticism that the Impact Team is actually serving as an anti-hero. Such behavior invites the question: can immoral means be justified in meeting a moral end?

The Impact Team issued an ultimatum to ALM’s direction that amounted to an extortion attempt. Should ALM elect not to concede to blackmailing by shutting down its business, they threatened to make public all customer records, including profiles, real names and addresses, employee documents, and e-mails. The last of these would include intimate details of customers’ secret sexual fantasies and information on whether any planned sexual encounter came to fruition. To demonstrate their ability to make good on their threat, the Impact Team released a sample of information detailing the company’s employee salaries and networking structure (Zetter, 2015).

ALM was clearly cognizant of its offering a service that flouted the norms of acceptable behavior. As the later data dump would reveal, thousands of the subscriber e-mail accounts bore .mil (military) and .gov (government) suffixes. The company recognized its own notoriety with openly bartering in infidelity. Its marketing strategy conscientiously leaned into the criticisms it was up against. With an attitude of there being no such thing as bad publicity, and the distinction between fame and infamy being a trivial one, in 2009 ALM attempted to purchase advertising during the Super Bowl. Their instincts on this were quickly vindicated. As word spread of their failed attempt to buy advertisement space, the unaired advertisement generated more than a million views on YouTube (Lee, 2015). To emphasize yet further its financial well-being and embrace of notoriety, the company also made a bid for the naming rights to the Meadowlands Stadium, home to the New York Jets and Giants.

ALM responded to the threat of organizational doxing (i.e. releasing private information into the public domain without or against the consent of those whose information is at risk) with two strategies. The first was to involve law enforcement efforts to combat the data breach, dubbing it cyberterrorism. The data were illegally obtained and individuals purchasing Ashley Madison’s services, as disreputable as many would find their behavior, have a legal right to privacy. The obvious limitation to the strategy is that the data had already been leaked by that point. The best that a police investigation could achieve would be to identify and punish the Impact Team criminally. That proactive approach was paired with a reactive one of purging their database of all personal identifiers. The company had been in the practice of selling a full delete option for USD 19. Given the crisis and the public relations hit it was being subjected to, it summarily waived that fee for any customer wishing to engage that option. The effort to purge their records after the breach proved ineffectual. The Impact Team made good on their threat to expose those actively attempting to cheat on their spouses. The records of millions of users hacked from Ashley Madison, complete with personal identifiers, were posted online for all to see. Given the salacious content, technological angle, and feel-good righteous retribution that Ashley Madison was receiving, the story became a media spectacle. The press reaction raised several questions connected to the business ethics of facilitating online dating.

What Protections Does a Provider Owe to Its Users?

A story such as this, bearing all the earmarks of a tabloid affair, aroused intense media interest. Readers wanted details of the case. The arc of the story followed that of nearly all other press accounts detailing data breaches. People want to know what level of risk they face when making online purchases. Our intention is to find ways to minimize exposure to having private information falling into the wrong hands. Part of the collective effort of the business and tech press was to detail the business practices that made Ashley Madison vulnerable. Much of what was discovered along the way indicated unscrupulous business practices, which perhaps only fed the schadenfreude of these media accounts.
The headlines that gained the most traction in the media were connected to the overall female presence on the site. More specifically, the initial analysis of the data indicated a minimal presence. As one might suspect, the site was used by an overwhelming majority of men. A number-crunching report by the tech publication *Gizmodo* indicated that only about 12,000 of the 5.5 million registered female accounts were consistently checked. That is equal to three for every 1,000, or less that 1% (Reed, 2015). For every one e-mail inbox check a woman ran, 12,585 men did the same. The plot thickened when the author noted a peculiarly high number of the female accounts were created from the same IP address.

The oddities raised by the pattern discovered above raised the question of just who or what was accounting for the scant female presence on the site. A closer inspection into the Impact Team’s data by *Gizmodo* revealed the following:

Equally clear is new evidence that Ashley Madison created more than 70,000 female bots to send male users millions of fake messages, hoping to create the illusion of a vast playland of available women. (Newitz, 2015)

In the *Gizmodo* write-up, Newitz presses the argument further:

What I have learned from examining the site’s source code is that Ashley Madison’s army of fembots appears to have been a sophisticated, deliberate, and lucrative fraud. The code tells the story of a company trying to weave the illusion that women on the site are plentiful and eager. Whatever the total real, active female Ashley Madison users is, the company was clearly on a desperate quest to design legions of fake women to interact with the men on the site. (Newitz, 2015; emphasis in original)

The allegations of fraud did not stop here, however. The full delete option it sold to its consumers was apparently offered under false pretenses as well. *The Verge* reported some disturbing findings of its practices with that option:

Ashley Madison’s hackers have already claimed that the site’s “delete everything” service, which charged its affairs-seeking users $19 to remove any trace of their presence on the site, wasn’t entirely effective. And now internal documents leaked as part of the massive breach have shown that the company profited heavily thanks to the disingenuous promise of “full delete”. According to *BuzzFeed News*, one memo points to Ashley Madison having made $1.7M in incremental revenue in 2014. (Welch, 2015)

Further, there is the matter of whether the company managed to cover up the digital footprints that would have been inevitably left for those many who elected to pay for the option with a credit card.

There are a few analogies to be drawn with more traditional online dating platforms, albeit with much less consequential stakes involved. There are tens of thousands of profiles housed by Tinder and OkCupid that are dormant. It is not entirely clear what their policies are on purging unused accounts. Is there a time frame at which point the dormant accounts are automatically deleted? Otherwise, users will be swiping on and directing messages to inert accounts. To the degree that ghost accounts exist, consumers are being sold on one experience only to be chasing a phantom. It is a little league version of being duped, Ashley Madison style.

The animating question is whether this is a straightforward case of *caveat emptor* or if the company legitimately owes greater transparency to its customer base. If the latter more than the former, the inquiry moves in the direction of what might be the best way in which to facilitate greater consumer oversight. Some might prefer the Federal Communications Commission (which until recently was promoting a net neutrality agenda) or some other similarly situated governmental entity to ensure a modicum of consumer protection for online transactions. The Better Business Bureau or some other Yelp-like entrepreneur could elect to allow consumer
ratings of the online provider. Yet another alternative would be for online providers to take it upon themselves
to ensure transparency. Perhaps a system that allows users to rate the service and verify their encounters
in real life with others on the site would be one way to crowdsource the task. Such a remedy would offer a
simple solution to weeding out those creating fake profiles to fish for business. Reforms such as these would
go some distance in separating the industry from the shame of the Ashley Madison business practices.

How Can Companies Mitigate Risks ARISING in Real Life From Activities Facili-
tated Through Online Connections?

In addition to the list of alleged crimes of commission, The Verge raised a few pointed questions over sins
of omission that Ashley Madison may have committed (Brandom, 2015). Engaging in actively seeking part-
ners with whom to engage in infidelity involves conveying sensitive information. There are indications that
Ashley Madison was decidedly less than careful with providing ironclad measures to ensure privacy. Much
of the problem relied on the site simply templating the security measures provided to other vendors such as
Amazon and Gmail. These measures proved inadequate for preventing identification while arranging for mar-
tial infidelity. For example, an inquisitive spouse can determine whether her husband is on the site merely by
plugging his e-mail into it to see whether it is a recognized account. The site also followed standard proto-
col in housing real names and addresses on file to ease the bill collection on account of the sensitive nature
of contracting in infidelity. Carelessly neglecting to fortify its security with a few simple measures cost many
clients their reputations with the data hack.

The list of celebrities in the data dump provided yet more fodder to feed the media curiosity with the story.
Among the biggest names were Josh Duggar and Snookie’s husband. Both Duggar and Snookie were reality
TV stars. Josh Duggar appeared in 18 Kids and Counting, detailing the life of a Christian fundamentalist fam-
ily with an exceptionally large family. Snookie starred in the MTV show The Jersey Shore, which followed a
co-ed group of 20-somethings living the summer party in a vacation spot. The former had his reputation suffer
considerably more than the latter but both lost credibility as the scandal undermined their public personas.
The reputational damage was particularly acute in the faith community. John Gibson, a Baptist minister in
New Orleans and Hamza Tzortzis, a leading public speaker on Islam in the UK, were found in the data dump.
Subsequently, Gibson explicitly referenced Ashley Madison in his suicide note.

There were less acute reactions that caused turmoil of various degrees. Firstly, there were the families of
those registered on the site. In the aftermath there were sites constructed that permitted user-friendly search-
es, meaning that anyone could determine whether their neighbor was planning or actively engaged in adul-
tery. It served to make private family problems public domain. A closer look at the data (Newitz, 2015) also
revealed whether individuals were seeking to engage in marital threesomes or same sex partnerships; again,
making the private public would make for awkward encounters and fractured relationships. Lastly, there were
those whose names appeared in the data dump that were pseudonyms. Some, such as Al Capone, Taylor
Swift, Hitler, Martha Stewart, Pope Francis, and Barack Obama, who is included in numerous entries, are ob-
vious fakes. In the meantime, many were not waiting to do due diligence in verifying identities. There was a
brief wave of crime targeting those on the list for extortion attempts. People with public reputations for being
upstanding might pay such a ransom to maintain good standing after all.

The content above raises the matter of how privacy ought to be handled. More specifically, what happens
to all the correspondence that is generated on Web-based dating platforms? Providers that do a better job
of connecting consumers will control a greater share of the market. Gaining that advantage will require their
analyzing the data generated by their users to optimize the algorithms it uses to distribute content. Answer-
ing questions that detail sexual tastes (as OkCupid does) and tracking intimate correspondence is eligible for
hacking and extortion as well. Perhaps pay sites like Match.com and Eharmony should begin implementing
safety measures like recording their patrons and their records under pseudonyms. For those wishing for a
failsafe, foolproof insurance in putting all identifying data beyond the reach of hackers, there is always the
option of paying in cryptocurrency such as Bitcoin. It bears mentioning that every Web dating service caters to clients actively engaged in cheating. They are simply less forward than Ashley Madison in acknowledging, much less promoting, the behavior.

The reason privacy matters is that the repercussions stretch beyond cyberspace into reality. How much vetting of potential users of a site does the company owe to existing members? These kinds of issues come to the fore in extreme cases such as the Craigslist killer who targeted his victims through the singles advertisements on the site. There are other less horrifying but problematic results that go beyond an awkward date which could result from misinformation being posted in an online profile. Setting just the right amount of verification to qualify as a legitimate farmer on Farmersonly.com or Christian according to Christian Mingle is a judgment call. But clearly, as the Craigslist killings indicate, there is not just a potential moral obligation to protect users, but also a business interest in avoiding the ignominy of such negative press these instances bring about.

Discussion Questions

1. What might be done to introduce more transparency into online dating?
2. What protections do online providers owe to their users?
3. What might you suggest as an optimal strategy for ensuring privacy?
4. Are there practical measures vendors might provide to offer some measure of quality assurance?

Additional Material

Fembots on Ashley Madison (YouTube): https://www.youtube.com/watch?time_continue=2&v=FVQw58Pt_R8

References