

An Ethical Dilemma: A Case Study of the 2015 Ashley Madison Data Breach

Leisl Seigler

Department of Communication Studies

lseigler@samford.edu

Abstract

This is a case study outlining the timeline of the 2015 Ashley Madison data breach. It discusses Noel Biderman's part in the downfall of Ashley Madison, the organizational culture of Ashley Madison, and the ethical dilemma both inside and outside the organization. It looks through the lens of Organizational Communication at the interworking of the world's largest infidelity website. Implications for future hacks are also given.

An Ethical Dilemma: A Case Study of the 2015 Ashley Madison Data Breach

History of Ashley Madison

Based in Canada, Ashley Madison (AM) is an online dating service, marketed specifically for people who are married and looking for extramarital affairs. Founded in 2001 by Noel Biderman and owned by Avid Life Media (ALM), AM had a swift rise to success. By 2006, AM claimed to have 1.1 million members, spanning 37 countries (Roast Beef TV). After appearing to have survived the 2008 recession, AM announced a gross income of \$115 million in 2014; a total increase of 45% in one year (Roast Beef TV, 2016). With AM's rise to fame came an interest in the man who founded AM and kept it going.

Noel Biderman

Native of Toronto, Canada and grandson of Holocaust survivors, Noel Biderman is a Jewish businessman (Price, 2015). Biderman has an undergraduate degree in economics from the University of California and a law degree from Osgoode Hall Law School in Toronto (Price, 2015). The idea for AM came from his business in the sports world, where Biderman represented athletes in infidelity scandals (Price, 2015). Biderman has written multiple books about infidelity, including "Cheaters Prosper: How Infidelity will Save the Modern Marriage" in 2011 (Price, 2015).

A husband and father of two, Biderman founded and helped run a myriad of online dating sites, including AM, Established Men, and Cougar Life (Roast Beef TV, 2016). Referring to himself as "the king of infidelity" (The Telegraph Journal, 2015) and "the Google of affairs" (Roast Beef TV, 2016), Biderman created an image of a caring CEO whose only goal was to help other people be happy in their marriages. He explained that just as Google did not invent "looking stuff up," but it made it easier, he did the same with affairs. He claimed that infidelity

saved marriages (Roast Beef TV, 2016) and that while he himself would never even consider having an affair, other people did and his site could help those people be happy.

Biderman was a master of marketing, both for himself and for his controversial companies.

Much of this success can be attributed to Biderman's clever marketing scheme. AM's marketing teams consistently produced provocative ads that were often banned from websites, billboards, and even entire countries. The removal of the ads usually caused a media stir, indirectly encouraging people to look up the banned advertisements online. Thus, AM received more members through completely free advertisement simply by being provocative (Roast Beef TV, 2016).

Biderman's most interesting marketing ploy, however, was including his wife in not only interviews about AM, but also in advertisements themselves. Amanda appeared as the model on multiple billboards and commercials for AM (Roast Beef TV, 2016). She constantly showed her support of her husband's business, though she was quoted as saying that she would be angry if she found that he used a site like AM (Roast Beef TV, 2016). Biderman used his dynamic personality and marketing skills to create the massive company that was AM.

The 2015 Data Breach

Timeline

In July of 2015, however, Biderman's world came crashing down. On July 18, AM employees opened their computers to find an intimidating message from a team of hackers called The Impact Team (Bisson, 2015). Claiming that the team had successfully hacked AM's data storage, The Impact Team demanded that AM and Established Men be shut down immediately or the team would release all of the identifiable information onto the public web (Bisson, 2015). Biderman refused to shut the sites down and put his technology team to work closing the

breaches in the data vaults.

True to their word, on July 19 The Impact Team sent the same manifesto out to the public (Bisson, 2015). Initially reported by Brian Krebs, the hackers explained to the public that if Biderman did not shut down AM and Established Men within 30 days, they would release all the information onto the web (Krebs, 2015). Biderman responded the same day in a press release, acknowledging the hack as legitimate and explaining that “the company [was] working diligently and feverishly” to close the breaches and regain the stolen information (Krebs, 2015).

After 30 days, however, it was clear that AM had either lied about the intensity of its efforts or had failed. On August 18, 30 million user profiles were dumped onto the dark web, including identifiable information such as emails, credit card information, full names, and exchanged messages (Bisson, 2015). On August 20, just two days later, a second data dump of about the same size was released (Bisson, 2015). Lastly, on August 22, a third data dump was released (Bisson, 2015). This last dump, however, was not user profiles; it was internal documents of AM itself (Bisson, 2015). These internal documents included everything from the business practices to private emails of employees, including those of Biderman.

On the heels of these data dumps, AM announced on August 28 that Noel Biderman was stepping down as CEO, “effective immediately” (The Telegraph Journal, 2015). Despite the uproar in the media, on August 31, AM reported that since the hack, 90,000 new members had joined the site and that 2.8 million women had exchanged messages with other users on the site in the weeks following the data dumps (Covert, 2015; Bisson, 2015).

The Impact Team

No one is sure who the Impact Team is, though the team itself is comprised of highly skilled and experienced hackers (Cox, 2015). Biderman suggested at one point that it was an

inside job, an employee or former employee who had access to the company internally (Krebs, 2015). The manifesto sent out by the hackers online and to employees seems to support this idea. For example, the manifesto mentions Trevor Stokes, ALM's chief technology officer (Krebs, 2015) by name and title: "Protection of personal information was [Trevor's] biggest critical success factors and [he] would hate to see [AM's] systems hacked and/or the leak of personal information. Well Trevor, welcome to your biggest fucking nightmare" (McLellan, 2015). The team also mentions Mark Steele, AM's director of security, by name in the manifesto (McLellan, 2015).

The Impact Team claimed that the hack was easy. When asked by Joseph Cox (2015) of Motherboard what the security of AM was like, the Impact Team reported that it was "bad. Nobody was watching. No security" (Cox, 2015; McLellan, 2015). The team further explained in both the manifesto and to Cox that the hackers had been gathering information from AM for years (Cox, 2015; McLellan, 2015). The hackers also indicated that although they put much effort into making the hack undetectable, once inside, they found no security measures that would have given them away (Cox, 2015).

Another theory about The Impact Team's identity is that a disgruntled spouse hacked or hired someone to hack the site. However, the motives of The Impact Team do not match the expected motive of a betrayed spouse. The Impact Team's main motive was to expose AM for fraud, not to uncover cheaters. In the interview with Motherboard, The Impact Team explained that to understand what was really going on at AM, they had to watch the site internally for years (Cox, 2015). They found that AM was storing identifiable user information, even though the site boasted a full delete account option. After watching millions of users sign up for a fraudulent service, the hackers decided to step in to save others from joining such a fraudulent organization

(Cox, 2015). They likened AM and ALM to “a drug dealer abusing addicts” (Cox, 2015). In the manifesto, the team explicitly attacked AM’s full delete option for a \$19 charge. This option is a huge money maker for AM, as it promises that the user’s name, information, email, sexual fantasies, credit card information, etc. will be completely erased from AM’s records forever. The hackers discovered, however, that this was a lie and that the information was still stored in AM’s data troves (McLellan, 2015).

Although The Impact Team told Motherboard that they would hack any site or person who made millions on fraudulent claims, the hackers disappeared after the AM hack of 2015. If the team has been involved in other hacks, it has not attached its name to those hacks (Roast Beef TV, 2016). Furthermore, there has not been a hack like this since 2015. Many hackers seek identifiable information to help themselves and privately stow away stolen information. These hackers, however, stole and publically released everything they had on users and the company, making this hack especially notable (Roast Beef TV, 2016).

Resulting Lawsuits

The 2015 hack and the accusations made by The Impact Team launched many class-action lawsuits against AM and ALM. The largest lawsuit against ALM, seeking financial compensation of \$576 million for the “people affected by the breach,” was filed by Canadian law firms Charney Lawyers and Sutts, Strosberg LLP (BBC, 2015). However, most prominent and incriminating in the onslaught of lawsuits and investigations against ALM is the Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner, published to the public on August 22, 2016.

First, the investigations into AM’s security precautions were found to be lacking in three

ways: AM did not foster a privacy or security aware culture through training or management courses; AM did not have “an explicit risk management process” or briefings about potential breaches or privacy threats; and AM did not have adequate training programs for all staff that would teach employees what their obligations for security were in the company (Office of the Australian Information Commissioner, & Privacy Commissioner of Canada, 2016).

Second, while privacy laws in Australia and Canada do require businesses to store information for “as long as necessary to fulfil the purpose for which the personal information was collected” (Office of the Australian Information Commissioner, & Privacy Commissioner of Canada, 2016), ALM failed to communicate this to its users. ALM attempted to justify retaining personal information in case a user wanted to reactivate his/her account, but the investigation concluded that the low rate of users who did this did not justify the need for retaining personal records indefinitely. Privacy laws require businesses to personally determine a reasonable retention time of information and to communicate that time with their customers. ALM failed to do this with AM users, and thus, was in violation of privacy and consent laws (Kratz, 2016).

Third, the investigation discovered that ALM was in violation of laws requiring businesses to be open and transparent with their customers. ALM fabricated a “trusted security award” on their website, though this award does not exist (Brownwell, 2016; Office of the Australian Information Commissioner, & Privacy Commissioner of Canada, 2016). Furthermore, the terms and conditions of AM’s website are unclear and confusing to the average reader, regarding the retention of identifiable information. Lastly, only after the \$19 full delete charge was paid were users informed that their information would be retained by the company for “at least” 12 months. Thus, ALM violated consent and data storage laws (Office of the Australian Information Commissioner, & Privacy Commissioner of Canada, 2016). These findings indicate

that AM was guilty of both false advertisement for the \$19 full delete option and false advertisement of security measures, as well as improper storage of identifiable information and failure to protect that information.

AM and ALM were guilty of another form of false advertisement, as well. In 2013, Elie Mystal reported in Canadian law website, *Above the Law*, that ALM was sued by a former employee of AM for “unjust enrichment at her expense,” seeking \$20 million (Mystal, 2013). Doriana Silva was hired by AM to help launch the site in Portuguese, but was asked to create over 1,000 fake female accounts for the company to use to lure in men, otherwise known as fembots (Mystal, 2013). Deeply embedded in the terms and conditions listed on AM’s website is one clause that states that by becoming a member of AM, “you acknowledge and agree that some of the profiles on the site...may be fictitious” (Mystal, 2013). AM still, though, charges customers to pay to chat with these fake accounts that its own employees mass produce so that they make more money. Although they are protected, it is still fraudulent.

The Culture of AM

Many people wonder how a person could possibly justify working for or participating in an organization which exists for the sole purpose of finding an affair. But AM was/is a genius at creating an image that distorted what it truly stands for.

Biderman’s Seemingly Pure Image

Noel Biderman made himself seem like a loving husband who created a website to help people. He believed that people were going to have affairs anyway, so he was simply making it more private and less embarrassing for cheaters. He separated himself from the purpose of his website(s) so well that his employees, his wife, and the site’s users were disillusioned with AM’s true intentions. When asked how she felt about her husband’s business, Amanda replied: “Really,

the business itself doesn't match who he is as a person — it's not our lifestyle or value system or any of that” (Kolhatkar, 2011). Furthermore, during an interview with NBC news, Biderman checked his phone, commenting that his wife had called reminding him to take a cake to his son’s school for his birthday, a call he said he “like[s] to return” (Kolhatkar, 2011). The statements made in this interview demonstrate the amount of effort Biderman put into creating a good image of himself.

Treatment of Employees and Power

Additionally, employees likely did/do not think of AM for the bigger picture, but rather only in terms of their specific job, which in many cases probably has nothing to do directly with finding affair partners for people. Being so focused on their small job at such a large organization and having an outspoken and charismatic CEO kept employees from seeing AM for an affair site. Another former employee of AM, Louise Van Der Velde who was hired by AM as a media spokesperson in 2013, indicated in a documentary that AM treated its employees poorly. Following a financial dispute, she fell out of favor with the company and quit shortly after. She believed that AM treated its employees so poorly that The Impact Team was likely an employee who had been bullied or mistreated so badly, he/she decided to ruin the company forever (Roast Beef TV, 2016). If employees were mistreated or afraid for their jobs, they may have never questioned their role in the unethical company because they were solely focused on keeping their jobs. This fear could also keep employees from exposing the company of fraud if they knew about it. Mistreatment of employees and the resulting fear is likely a cause of a large power gap between employees and their superiors.

Slogans and Symbols

It takes incredible marketing skills to sell an affair service to so many people, but AM’s

marketing team excelled and continues to excel at doing just that. When AM first appeared on the web, its slogan was “Life is short. Have an affair.” This slogan appeals to a *carpe diem* lifestyle. The underlying beliefs that accompany that slogan are that affairs are short lived and are not serious, but neither is marriage. Life is short. Why waste it with one person? Any person already even mildly dissatisfied with his/her marriage could read that slogan and immediately buy into what it was truly saying and then justify any resulting cognitive dissonance using the beliefs of the slogan.

Additionally, the symbol of AM was initially a fallen wedding ring that made the “o” in “Madison.” The fallen ring most clearly shows what AM’s true purpose was: to find an affair. But this logo is just subtle enough that it is easy to overlook. It is part of the name of the site. It is not set apart in any way, nor is it shown on a person’s hand. It subtly lies there, in the same color as the words “Ashley Madison,” shown below in Figure 1.

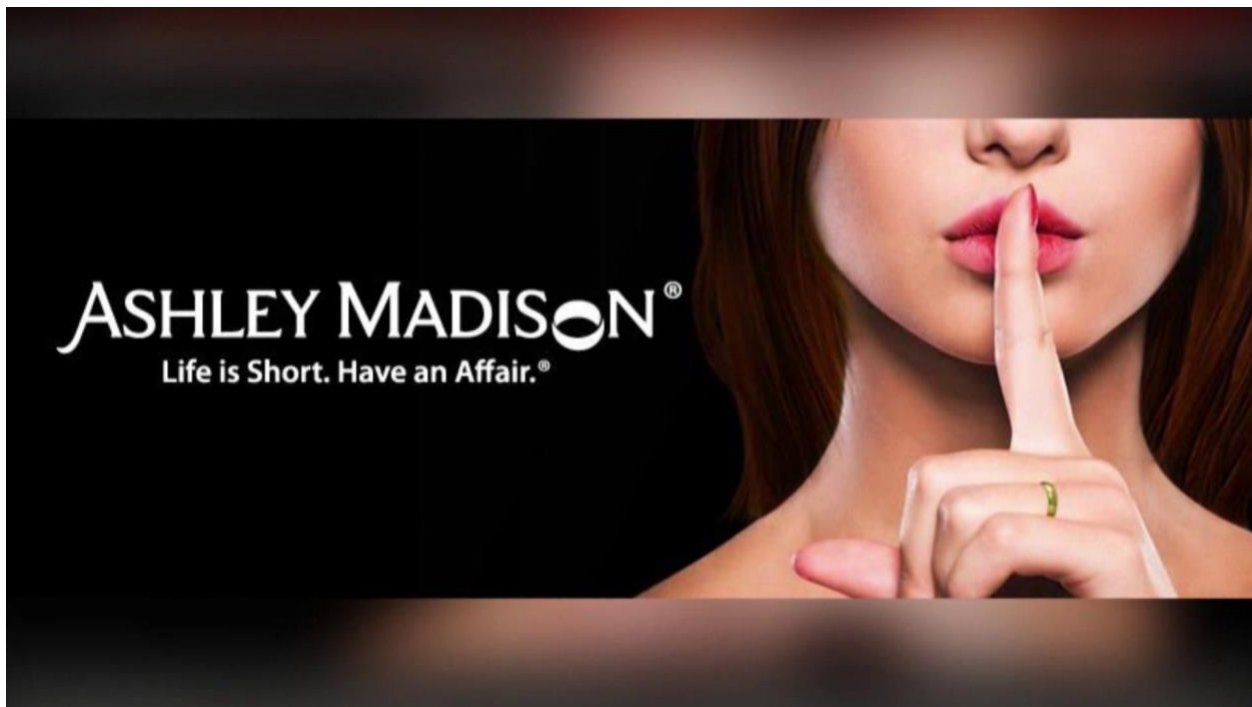


Figure 1: Former AM logo from the AM website.

In many commercials for AM, the ring actually falls out of the word “Madison” and makes a

clinking sound, as if it is falling against a hard surface. But only in these commercials is the ring that obvious. The ring also indicates AM's intended audience: married people. Prior to the hack, AM never marketed itself as a place for singles. It was a place for consenting, married adults, who wanted fun and secrecy for a short time, to gather and experience just that.

Descriptions of the Organization

In conjunction with these slogans and symbols, AM's leadership described the organization as a place of "exploration." A purposely ambiguous term, the leadership of AM wanted people to believe that the site was not simply a place for affairs, even though that was its goal at heart. It was marketed as a place where a person could find anything from a texting romance to a full-fledged affair. It was a place where adults could find what they liked sexually without any pressures from their partners to like or dislike certain fantasies.

It was further marketed a place designed for entertainment purposes only. This is how AM justified its use of fembots. People were not supposed to take the site that seriously. AM was marketed as never being created to encourage real affairs. It was simply supposed to give people, mainly men, a good time without including their partner. These "fake" affairs were also not long term or detrimental to people's relationships. As one former AM user explained: "They made it sound like it was this play land of people hooking up" (Roast Beef TV, 2016). Another user described the site as a "quick hook up kind of site" (Roast Beef TV, 2016).

AM was/is also marketed as a site for any type of relationship. AM often called these "discrete relationships." This description was an attempt to show AM less as an affair site, which has a strongly negative connotation, and more of a site for any type of stigmatized relationship, which has a more positive connotation. For example, the website states that AM is great for exploring work or homosexual relationships (Ashley Madison).

The Ethical Dilemma

Despite AM's effective marketing strategies and seemingly spotless CEO, the 2015 hack exposed AM for deception on every level of the organization.

Internal Ethical Dilemmas

Security Concerns Prior to the Hack

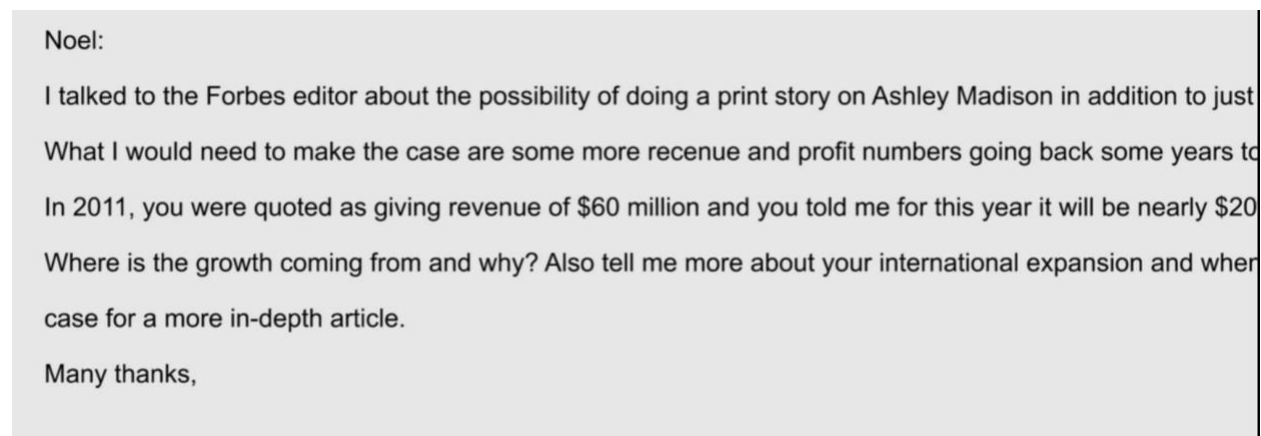
Leaked internal documents from the hack revealed that prior to the hack, employees were sent a questionnaire that asked them to express their greatest concern as a worker at AM/ALM. Many employees indicated that they were most concerned with an error in security. Ironically in the questionnaire, Trevor Stokes explained that he specifically "would hate to see [Ashley Madison's] systems hacked and/or the leak of personal information" (Krebs, 2015). Furthermore, in early 2015, just a few months before AM was hacked, AdultFriendFinder.com was hacked, causing concern for AM's safety (Krebs, 2015). *The Wall Street Journal*, in fact, wrote an article in May of 2015, barely two months before the data breach, entitled "Risky Business for AshleyMadison.com" that speculated about the likelihood of a data breach at AM: "given its business's reliance on confidentiality, prospective Ashley Madison investors should hope it has sufficiently, er, girded its loins" (Krebs, 2015).

Biderman's True Colors

Although Noel Biderman created an image of a caring and loving husband, the data breach revealed that he was a deceptive man and CEO. First, Biderman had a reoccurring habit of lying. In one interview, Biderman explained that sometimes prostitutes and escorts found their way onto AM to solicit business, but said that "I remove anybody soliciting. We try really hard. We are not interested in that" (Kolhatkar, 2011). However, the data breach revealed that Biderman and his companies, including but not limited to AM, actively encouraged solicitation

(Roast Beef TV, 2016). ALM, again, used its marketing skills to solicit escorts, calling their services “intimacy with a twist” (Roast Beef TV, 2016).

Furthermore, the data dump that included company emails revealed that Biderman explicitly told AM’s financial department to inflate financial data to ensure that magazines, like Forbes, would run articles on AM’s success (Roast Beef TV, 2016). In the documentary “Ashley Madison: Sex, Lies, and Cyber Attacks,” producers show screen shots of some emails recovered from the data breach. In those emails, a representative from Forbes requested more detailed records of revenue and profit, including the sources of the massive growth of the company, shown in Figure 2.



Noel:

I talked to the Forbes editor about the possibility of doing a print story on Ashley Madison in addition to just
What I would need to make the case are some more revenue and profit numbers going back some years to
In 2011, you were quoted as giving revenue of \$60 million and you told me for this year it will be nearly \$20
Where is the growth coming from and why? Also tell me more about your international expansion and when
case for a more in-depth article.

Many thanks,

Figure 2: Screen shot of email from data dump. Ashley Madison: Sex, Lies, and Cyber Attacks

In another email, an employee sent an email to Biderman with attached data “except the survey data which is large made up by pr” (Roast Beef TV, 2016) for the Forbes article. Other emails indicating deception of the media show that he further fabricated stories for an interview with Nightline about Cougar Life users. In Figure 3, the email between Biderman and his employee demonstrate that the story the female user was going to tell would be largely fabricated, similar to another story about Established Men. Biderman’s goal was to sell stock in AM on the New York Stock Exchange (Roast Beef TV, 2016) and on the London Stock Exchange (Price, 2015).

Having articles about his company in magazines like Forbes was essential to achieving that goal, and Biderman was willing to do whatever it took to be successful.



From: [REDACTED] ☆
Subject: Fwd: CougarLife update
To: [REDACTED], Noel Biderman [REDACTED] ☆
Hey [REDACTED]
Please be very cautious and attention to detail regarding [REDACTED] and her blind date. If Nightline smells anything suspicious they will kill the whole thing.
When I did this for Established Men we did a lot of prep work and coaching of the couple as it needs to feel genuine...and they need to have back storie: corresponding before they decided to meet, what was the progression - emails, phone calls etc.) Remember we're also positioning [REDACTED] as the most p

Figure 3: Screen shot of email between Biderman and an employee showing fabricated information for a Nightline story. Ashley Madison: Sex, Lies, and Cyber Attacks

But arguably the most unethical lie Biderman consistently told was that he was faithful to his wife. The email data dump revealed that Biderman had at least three affairs, but it is possible that he had as many as eight through his own websites (Roast Beef TV, 2016). When The Impact Team dumped the files of emails, they attached a note with Biderman's emails that read, "Hey Noel, you can admit it's real now," referring to his affairs (Bleier, 2015). Two of the three affairs included financial compensation to the mistress or someone else related to her. Biderman promised one of the women a job interview with ALM and a "good 'signing bonus'" (Bleier, 2015). Biderman was previously quoted in an interview saying, "If I wanted to have an affair, I would have one" (Bleir, 2015). He also explained that because he and his wife were still in the early part of their marriage, ten years at the time, they were "incredibly communicative about [their] sexual needs" (Bleir, 2015). However, he also said that sex is not the number one benefit in their marriage. Thus, if he became unsatisfied sexually in their marriage, he would "cheat long before [he] would get a divorce" (Bleir, 2015) because giving up the life he and his wife had built would not be worth destroying just for sex.

Regardless of what Biderman said to the media, his main motive was the success of his company, no matter the cost; the ends always justified the means. This and the above examples

also demonstrate that his secondary motivation was deception. He consistently chose to deceive people rather than to grow his business honestly. Biderman was not a man of integrity, evidenced both in his deception about his personal life and in his business practices. His habit of deception crept into the business of AM, and with no one to keep him in check, caused the company many problems after the hack revealed his lies.

There is no evidence that Biderman consulted a team of employees when making decisions in his organization. Aside from instructing his technology department to work on closing the breaches, Biderman did not appear to consult even AM's CTO about the best course of action. He also released AM's first response to the public about the hack, indicating that AM likely did not have a crisis management team or a public relations manager. If AM did have either of these, it appears that they were not consulted. While there are some instances where centralized decision making is necessary (Conrad & Poole, 2012), it would have been more effective in this case to have a group decision. Because Biderman made himself the spokesperson for the company, all eyes were immediately on him and when his dark secrets were revealed, he could not run from the spot light he created for himself. In a group setting, he might have been able to diffuse some of his part in the dirty business practices of AM, at least to the public. Biderman should not have made himself the sole decision maker for his organization, before, during, or after the hack not only because he created an inescapable spotlight for himself, but also because a group could have saved AM from being so deeply unethical.

AM Itself

AM is, undoubtedly, based on an unethical principle. Most people agree that infidelity is wrong and certainly should not be encouraged. Not only is AM's purpose unethical, but so is its business practices. As mentioned previously, AM used fembots to lure male customers to the

site. Although protected by its terms and conditions, this practice is unethical because while AM justifies the use of fembots because the website is for “entertainment purposes only,” most people do not see it as entertainment only. One user, a serial mistress who used AM to find men looking for affairs, had many real affairs with married men (Roast Beef TV, 2016). Thus, it is clear that the users of the site believe and expect that a real woman is on the other end of the conversation. Another unethical facet of the fembots is that users had to pay to view messages from other users. If a person is contacted by an interested party, he/she must pay an additional fee to open that message. This is the case no matter how many users reach out to a person. Every user must pay the same price to open the initial message for the first user that ever contacts them as for the thousandth user. Evidence from the data dump shows that AM used fembots to send an automated message to men to make them spend money and open the message, while the man thinks the fembot is a real woman. This is unethical on multiple levels. First, charging an extra fee simply to open messages is an anomaly in the online dating world. In most organizations, users pay a one time or monthly fee that includes freely opening messages from other people. Second, it is unethical to market the site as being full of women ready to have affairs, while a large percentage of those “women” are computer programs used by the company to earn more money. It is unethical to market the site as a place to find affairs and then use fake female accounts to lure men in, simply to exploit them and make money.

Additionally, AM charged a \$19 full delete fee, which is unethical. If a user has already paid for the services of a website, a full delete option should be covered in the initial fee. For example, the popular online dating site, eHarmony, requires a monthly fee to use its services, with different packages that provide a range of benefits. The full package includes unlimited message exchanges, views of matches’ profiles, access to matches’ photos, etc. Also, included in

eHarmony's services is the option to close or delete user information for free at any time (eHarmony, 2000). It is abnormal for a site to charge a fee for deleting an account, even in the online dating realm.

Not only is the charge itself unethical, but AM's dealings with the "deleted" information were also unethical. Users were told that their data, including identifiable information, was deleted completely once the charge was paid. However, the data dump and the resulting investigation revealed that this was not the case. There is little evidence indicating that Biderman or the company kept this information for malicious reasons; they did not seem to have a motive to sell it or exploit users' information. The only slight indication that Biderman could have made the decision to keep user information for reasons other than a customer reactivating his/her account (pp. 8), was in an interview with *The London Evening Standard*. After referring to himself as "The Google of Cheating," Biderman added that "the data collected by Ashley Madison would help researchers study infidelity" (Bleier, 2015). However, data recovered in the hack neither confirms nor denies this statement. There is no indication that this is the true reason why AM kept information, nor that the information was used in research.

External Ethical Dilemmas

Regardless of the motives of the hackers or the crookedness of the target organization, secretly breaking into stored data, stealing it, and then releasing it to the public is a crime (Roast Beef TV, 2016). Likely, the hackers chose to hack AM, rather than go through a legal route, for an immediate response and for the shock value. Legal processes take much time and money, evidenced in the investigation by the Canadian and Australian governments that was published over a year after the hack (Office of the Australian Information Commissioner, & Privacy Commissioner of Canada, 2016). The hackers clearly wanted immediate results and action,

something they apparently felt they could not attain through the legal system. In a statement after the hack, ALM went so far as to call the hack “cyber-terrorism,” promising retribution for affected users (Krebs, 2015).

Many people saw The Impact Team’s actions as praise-worthy because the general population considers infidelity, much less marketed infidelity, wrong. The Impact Team used the sentiment of the masses to its advantage, using AM’s dishonest business as a justification for its own unethical actions. As a result, most of the uproar following the hack was directed at the people who used the site, rather than the hackers. People were grateful that justice came to spouses who would pay to have an affair, though shocked to find their favorite politicians, celebrities, and spouses in the data dump. Nonetheless, a cyber hack is unethical and illegal. In a statement following the hack, Biderman summarized the dichotomy between people’s feeling about AM and the ethics of the hack: “Like us or not, this is still a criminal act” (Krebs, 2015).

Another aspect of this external ethical dilemma is what companies should or should not do with employees who were found on the site. Famous for his appearance on his family’s hit television show “19 Kids and Counting,” Josh Duggar was among many whose user information was found in the data dump (Feinberg, 2015). He was soon fired from his position as executive director at Christian organization, Family Research Council (Feinberg, 2015). Although Duggar’s release likely stemmed from religious beliefs, it still raises the issue of whether or not companies should have power over their employees because of their personal life choices.

Aftermath and Recovery

AM handled the hack as well as can be expected for the size and type of data breach which it experienced. Initially, Noel Biderman served as AM’s spokesperson, which seemed to neither help nor harm the situation. Biderman acknowledged that the hack occurred and that they

were investigating the situation (Krebs, 2015). The rest of the company, however, did not seem to be on the same page as its CEO. A representative from *The Guardian* decided to call the customer support hotline ALM set up after the hack to delete her account which she created for a project (Hern, 2015). In total, she spoke with three representatives of AM, all of whom denied the success of the hack (Hern, 2015). They further asserted that AM's data storage was secure and that the media was making the situation seem worse than it was (Hern, 2015).

New Leadership

Shortly after the hack, though, ALM required Biderman to step down due to the first indications of his habit of lying (The Telegraph Journal, 2015). After Biderman's resignation, the company fell silent among the storm of lawsuits and investigations, until ALM announced new leadership for AM. Rob Segal was hired in 2016 as CEO of AM, along with new president, James Millership (Brownwell, 2016). Segal released an apology statement to the users affected by the data breach and announced AM's attempts at rebranding. This included a new narrative for the site: most of AM's users are single (Brownwell, 2016). Segal explained in an interview with *USA Today* "that his first step is to completely rebuild the company as a relevant, digital dating innovator that truly cares for our customers" (Bomey, 2016).

Rebranding

In addition to changing the narrative, AM changed its slogan to "Find your moment" because "'Life is short. Have an affair.' was a limiting label that's outdated and doesn't speak to the wide variety of connections people find on Ashley Madison" (Bomey, 2016). The former picture of a woman with her finger on her lips (Figure 1) has also been replaced with a less suggestive picture, featuring the new slogan (Figure 4).

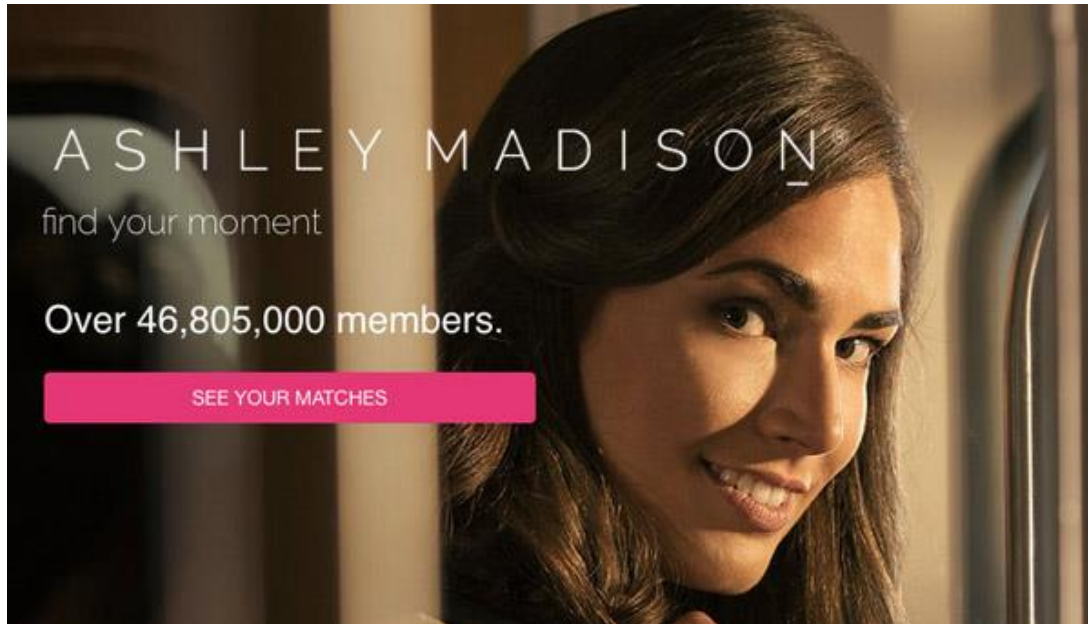


Figure 4: Current image and slogan from Ashleymadison.com

Lastly, ALM itself has rebranded to Ruby Corporation, with the ruby gem as its new emblem. In the “About” section of Ruby’s new website, the company is described as an “industry leader in innovative, open-minded dating services” (Ruby Life). It also explains that “[their] brands have grown to become household names,” a stark contrast with previous sentiments about a site for infidelity (Ruby Life). According to Millership, they chose the ruby because “it has a sensual feminine quality, connotes value” and fits the new image of ALM and AM (Bomey, 2016).

Implications and Suggestions for Other Websites

AM, however, is not the only company at risk. Other companies are now at greater risk than ever before due to the information hackers now target. Traditionally, organizations recognize three types of data as sensitive and of top priority to protect: payment card information, personal health information, and personally identifiable information (Tuttle, 2015). However, the AM hack indicates that hackers are now after “intellectual property” of users and companies (Tuttle, 2015). Intellectual property is intangible information, including information such as emails, personal preferences, biographies, etc., that is stored in tangible files. In the case

of AM, then, intellectual property is everything from the company's private emails to the sexual preferences of individual users. This shift in targeted information puts companies at greater risk of a data breach because the power the company holds is then shared by an, often, anonymous person or group. Companies gain power through controlling sensitive information (Conrad & Poole, 2012), and what hackers could or would do with intellectual property ranges from blackmail to selling it to competitors (Tuttle, 2015). Companies, such as Apple, have incredible power, as they have access to most or all their users' information. The access to all this information puts Apple and other companies at incredible risk for data breaches.

An example of a data breach involving intellectual property is the 2013 and 2014 hacks on Yahoo mail before the company was purchased by Verizon Wireless (Goel & Perlroth, 2016). Because Yahoo did not prioritize security of intellectual property, or data in general, and was hacked, the value of Yahoo dropped and Verizon purchased it for less than they had originally agreed upon (Goel & Perlroth, 2016). In this case, the hackers not only stole property from Yahoo, but also Yahoo's power.

An additional example of a company at great risk is Snapchat. Although it has not been hacked yet, the company has been suspected of storing its users' photos and *The New York Times* reported that someone discovered a way to recover photos shared on the app that were allegedly deleted, Snapchat's main marketing angle. (Shontell, 2013). If this is true, Snapchat itself has a high level of power because of the millions of indecent and incriminating photos it stores, while also putting itself at risk of losing its power and wealth in lying to its customers by claiming that all pictures "disappear" or are "deleted" after they are viewed. Thus, any hacker who stole this intellectual property would share Snapchat's position of power because Snapchat has much to lose. Hacktivism poses a particular hazard to companies that store the intellectual property many

hackers now seek, such as Snapchat. Online dating sites, pornography sites, Facebook, Instagram, Apple, etc. must now take extra precautions to protect the intellectual property of their users.

The AM data breach demonstrated that when information is controlled within a company, it is at least safe from being spread. However, in the hands of the wrong person, the power that intellectual property holds can be misused and devastating for users and companies. Thus, companies must expand the information which they deem most sensitive to include intellectual property and provide more security measures to protect their users.

References

- Ashley Madison. (n.d.). <https://www.ashleymadison.com/>
- BBC. (2015). Ashley Madison faces huge class-action lawsuit. *BBC News*.
<http://www.bbc.com/news/business-34032760>.
- Bisson, D. (2015). The Ashley Madison hack- a timeline. *The State of Security*.
<https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline/>
- Bleier, E. (2015). Ashley Madison founder's emails reveal he had multiple affairs despite his claims he never cheated on his wife. *Dailymail.com*.
<http://www.dailymail.co.uk/news/article-3212377/Emails-Noel-Biderman-Ashley-Madison-reveal-multiple-affairs-despite-claims-never-cheated-wife.html>
- Bomey, N. (2016). Ashley Madison's new slogan: 'find your moment,' not 'have an affair.' *USA Today*. <http://www.usatoday.com/story/money/2016/07/12/ashley-madison-avid-media-ruby/86981490/>
- Brownell, C. (2016). Ashley Madison probe finds deception, lax security. *National Post's Financial Post and FP Investing (Canada)*. Retrieved from LexisNexis Academic.
- Brownwell, C. (2016). New leadership team for Ashley Madison website; members apology for data breach. *North Bay Nugget*. Retrieved from LexisNexis Academic.
- Conrad, C. & Poole, M.S. (2012). *Strategic Organizational Communication in a Global Economy, 7th ed.* Wiley-Blackwell/John Wiley & Sons, Ltd.
- Covert, J. (2015). It cheated death we're alive, and women love us: Ashley Madison. *The New York Post*. Retrieved from LexisNexis Academic.
- Cox, J. (2015). Ashley Madison hackers speak out: 'nobody was watching.' *Motherboard*.

- https://motherboard.vice.com/en_us/article/ashley-madison-hackers-speak-out-nobody-was-watching.
- eHarmony. (2000). http://help-singles.eharmony.ca/app/answers/detail/a_id/4426/~/how-do-i-delete-my-account-information%3F
- Feinberg, A. (2015). Family values activist Josh Duggar had a paid Ashley Madison account. *Gawker*. <http://gawker.com/family-values-activist-josh-duggar-had-a-paid-ashley-ma-1725132091>.
- Goel, V. & Perlroth, N. (2016). Yahoo says 1 billion user accounts were hacked. *The New York Times*. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0
- Hern, A., Fishwick, C., & Weaver, M. (2015). Ashley Madison customer service in meltdown as site battles hack fallout. *The Guardian*. <https://www.theguardian.com/technology/2015/jul/21/ashley-madison-customer-service-meltdown-hack-fallout>
- Kolhatkar, S. (2011). Cheating Inc. *NBC News*. http://www.nbcnews.com/id/41583762/ns/business-us_business/t/cheating-inc/#.WP6n3FMrLLZ
- Kratz, M. (2016). Naughty secrets- findings in the Ashley Madison breach. *Slaw*. <http://www.slaw.ca/2016/09/28/naughty-secrets-findings-in-the-ashley-madison-breach/>
- Krebs, B. (2015). Online cheating site AshleyMadison hacked. *Krebs on Security*. <http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>
- McLellan, D. (2015). The Impact Team manifesto to AshleyMadison.com. *Medium.com*. <https://www.theguardian.com/technology/2015/jul/21/ashley-madison-customer-service-meltdown-hack-fallout>
- Mystal, E. (2013). Ashley Madison should take better care of the females it hires to trick you.

Above the Law. <http://abovethelaw.com/2013/11/ashley-madison-should-take-better-care-of-the-females-it-hires-to-trick-you/>

Office of the Australian Information Commissioner, & Privacy Commissioner of Canada.

(2016). Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner. <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/ashley-madison?>

Price, R. (2015). The strange rise and sudden fall of Noel Biderman, the former CEO of Ashley Madison. *Business Insider*. <http://www.businessinsider.com/noel-biderman-rise-fall-ashley-madison-avid-life-media-2015-8/#born-in-1971-biderman-is-a-toronto-native-the-grandson-of-holocaust-survivors-he-is-jewish--although-unsurprisingly-he-thinks-the-10-commandments-are-outdated-1>

Roast Beef TV (producer) & Marking, H. (director). (2016). Ashley Madison: sex, lies, and cyber attacks (motion picture). The United Kingdom: Roast Beef TV.

Ruby Life. (n.d.) <https://www.rubylife.com/>

Shontell, A. (2013). Actually, Snapchat doesn't delete your private pictures and someone found a way to resurface them. *Business Insider*. <http://www.businessinsider.com/snapchat-doesnt-delete-your-private-pictures-2013-5>

The Telegraph-Journal (New Brunswick). (2015). Ashley Madison founder laves company after hack. *The Telegraph-Journal (New Brunswick)*. Retrieved from LexisNexis Academic.

Tuttle, H. (2015). Implications of the Ashley Madison hack. *Risk Management*.

<http://www.rmmagazine.com/2015/10/01/implications-of-the-ashley-madison-hack/>