Ashley Madison Data Breach of July 2015: Determining Moral Responsibility with Actor-Network Theory and Conditions of Responsibility Framework

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Neha Krishnakumar

May 13, 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISOR

Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

During the Ashley Madison Data Breach of July 2015, 36 million users' profile information was leaked to the public (Staff in the Office of Technology and the Division of Privacy and Identity Protection, 2016). Being a site that allowed members to commit extramarital affairs, the leakage of this data caused suicide (Jones, 2017). Few research scholars have analyzed this case in a scholarly sense, and those that did included legal and media-studies-related analyses that either implicitly held accountable Ruby Corp as a business for failing to preserve the privacy of its users (Jones, 2017), or decided against blaming the user for utilizing the site (Cross et al., 2018). These arguments, however, fail to determine who is morally responsible for this breach. Each stakeholder must be taken into account when determining who is morally responsible for this breach, and this is especially crucial to prevent further breaches and suicides from occurring again.

The Ashley Madison data breach was fundamentally caused by Ruby Corp, which is morally responsible because the company meets all the necessary conditions for responsibility: wrongdoing, causal contribution, foreseeability, and freedom of action. To analyze the moral responsibility of every entity, I will first identify every single primary actor according to Actor-Network Theory, and then I will use the four conditions of responsibility outlined above to analyze the responsibility of each actor involved. Actor-Network Theory studies networks comprised of diverse human and non-human actors assembled by a network builder to solve a problem or accomplish a goal. The conditions for responsibility consist of wrongdoing, casual contribution, foreseeability, and freedom of action. I will examine arguments and facts as part of primary, non-scholarly sources and secondary sources as a part of my argument.

Literature Review

While the Ashley Madison breach is common knowledge to those who have taken a cybersecurity course or are involved in the field, there exists a minimal amount of scholarly literature relating to the case. The paucity of analyses of this breach has focused on interdisciplinary elements of the repercussions of the case, and have been related to legal and media studies, examining the consequences of the breach for Ruby Corp and Ashley Madison users. However, the analyses of these cases fail to account for the actions of all of the actors in the network from a formalized ethical perspective.

In *Having an Affair May Shorten Your Life: The Ashley Madison Suicides* by Sakinah Jones (2017), the background of the Ashley Madison case, in particular the suicides that resulted from it was first examined. Next, Jones describes the legal precedent and how this case differs from existing precedent in tort legislation as it pertains to privacy law. Then, she argues for creating a solution that will benefit those who were harmed by the suicides in data-breach-specific cases, using the Ashley Madison case and the backlash as a case study. Finally, she implores businesses to respond to data security breaches through a statutory remedy.

In *Media Discourses Surrounding Non-Ideal Victims: The Case of the Ashley Madison Data Breach* by Cassandra Cross, Megan Parker, and Daniel Sansom (2018), the three authors analyze the Ashley Madison breach from a different angle: media studies. In particular, the way the media reported on the Ashley Madison case was discussed in detail. Cross et al. note that being associated with the website by any means, as well as taking any actions on the website, were two factors that were perceived as necessitating a guilty verdict by the media for anyone who used the site. Cross et al. argue that victim blaming was ever-present due to the "perceived immorality" of the website, and less because of the actions of the hackers that compromised the privacy of the members of the website.

While the second analysis discusses it from a different angle than the first, both present that the Ashley Madison case could have been handled differently. In addition, both cases discuss privacy, almost from a proto-ethical perspective. It is imperative to consider the ethical elements of the data breach in great detail. A formalized understanding of the ethics of the Ashley Madison case, particularly relating to the actions of all of the entities present in the case, could inspire new legal and media studies developments, among other fields. Actor-network theory and the conditions of responsibility framework will create a formalized basis to define and understand the actions of the actors involved in this incident. This paper will thus use an analysis using the qualities of wrongdoing, causal contribution, foreseeability, and freedom of action to understand the morality of the actors involved in the Ashley Madison case.

Conceptual Framework

The morality of the actors' actions in the Ashley Madison case can be analyzed through actor-network theory and the conditions of responsibility framework. Multiple sociologists conceptualized actor-network theory: Michel Callon, Bruno Latour, and John Law, all working on this framework during the 1980s and 1990s (Cressman, 2009), and the theory studies networks with human and non-human actors assembled by a network builder to solve a problem (Cressman, 2009). An actor can include any element of the system, while a network in actor-network theory can be a collection of actors but it is also, in effect, an actor itself (Cressman, 2009). In my analysis, I will find the primary actors that represent the network.

After identifying the primary actors involved, I will identify which actors are morally responsible for the case by analyzing the actions of the actors against the van de Poel and Royakkers (2023) model of four Conditions of Responsibility: **wrongdoing**: violation of a norm, **causal contribution**: performing or failing to perform a needed action, **foreseeability:**

knowledge of consequences ahead of time, and **freedom of action:** or lack of compulsion in acting. With these four conditions met, we can conclude that an actor is morally responsible. It is crucial to use actor-network theory, to identify the primary actors, and it is imperative to use conditions of responsibility to successfully organize our thoughts concerning the morality of the actions of all of the actors involved in the Ashley Madison case of July 2015.

Methodology

In terms of methodology, for my analysis of the wrongdoing of Ruby Corp, I decided to use the GovInfo Application Programming Interface (API) to examine the data through GET requests and POST requests ("GovInfo API"). An API is typically used to gather or update information, thus, I used the GovInfo API to examine data from collections or packages of legislation to determine the existence and frequency of data privacy-related legislation. Below, in Fig. 1, is the formatted query that I used for my wrongdoing analysis, along with some of the results of such a query in Fig. 2.

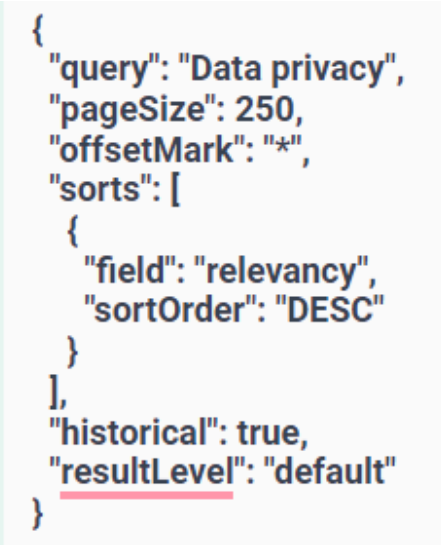

Fig. 1: Formatted Query for Wrongdoing Analysis

Fig. 2: Sample Result of Data Privacy Query

Analysis

Actor-Network Theory Analysis

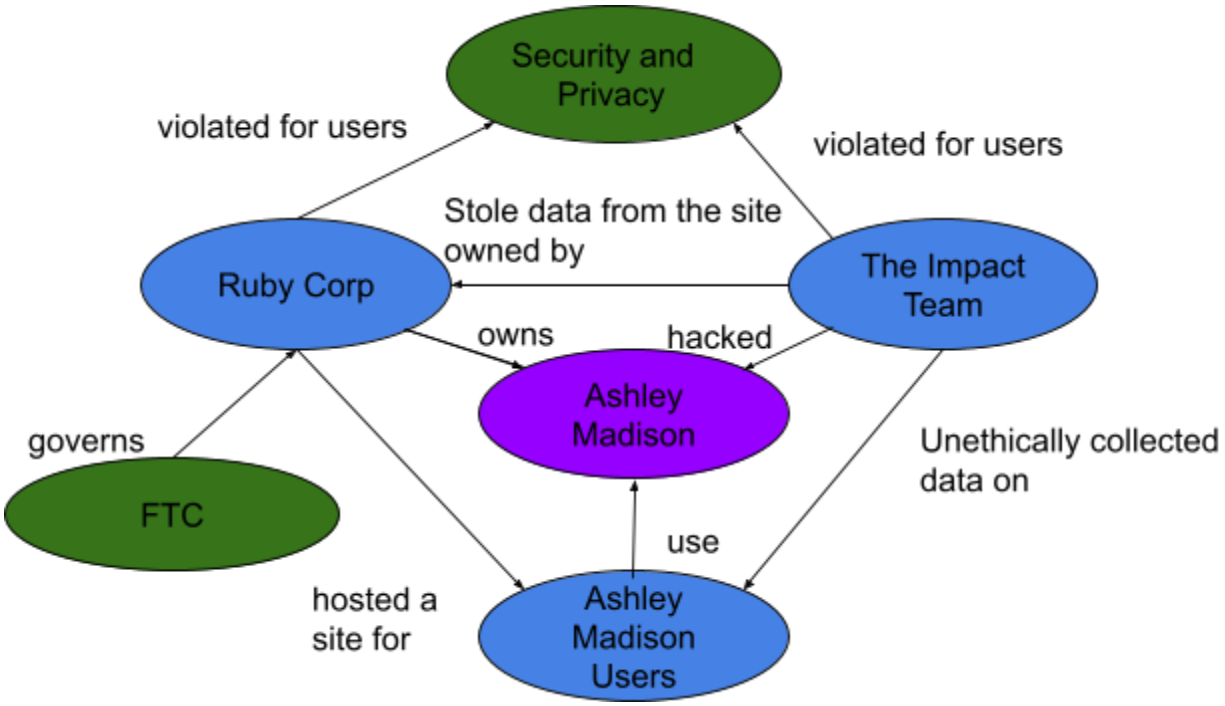

Fig. 3: Actor-Network Theory Analysis Graph

Above is a graph that includes all of the actors involved in this case as well as the relationships between the actors. The primary actors involved in this case are the users of Ashley Madison, Ruby Corp, the owner of the Ashley Madison system, and The Impact Team. The network builder involved in this case is Ashley Madison as the system was the one that had the

vulnerabilities allowing the data breach to occur. I will only focus on the primary, non-technical actors that count as representatives, because, although all of the actors, both human and non-human, bear some responsibility for the breach, only the human actors can be considered morally culpable. Thus, the aforementioned three actors will be considered for moral culpability based on the conditions of responsibility: wrong-doing, causal contribution, foreseeability, and freedom of action.

Conditions of Responsibility Implementation

The conditions of responsibility will be based on the conditions of wrongdoing, causal contribution, foreseeability, and freedom of action, which will all be assessed for the actors described above. Each section will define each condition of responsibility, followed by its application to the Ashley Madison case. Each condition of responsibility will be applied to each of the three primary actors in the Ashley Madison data breach.

Wrongdoing

Wrongdoing means violating a norm (van de Poel and Royakkers, 2023). In the Ashley Madison data breach of July 2015, there were two types of norm violations - violations of a law set by an existing regulatory body, specifically, the Federal Trade Commission (FTC), and violations of the implicit, ethically defined law of protecting the data privacy of Ashley Madison users. The primary actor involved in the wrongdoing was Ruby Corp, with the secondary involvement of The Impact Team.

Ruby Corp committed several violations of regulatory norms, particularly those set by the FTC. In particular, the settlement reached with Ruby Corp and the FTC identified a lack of an information security policy, reasonable access controls, poor security training, a lack of understanding of third-party security features and controls, and no measures to assess system

security (Staff in the Office of Technology and the Division of Privacy and Identity Protection, 2016). It is important to note that what was identified in the FTC complaint is not explicitly stated as a regulation by the FTC. The FTC, similar to the Supreme Court, does not create regulation - it enforces existing regulation, specifically in terms of data security as this example was. It is known that these regulatory norms were violated - but these existed as part of a complaint or a case. To truly examine if Ruby Corp committed any regulatory wrongdoing here, it is necessary to examine whether these laws existed in the first place, in the sense that the FTC as a regulatory body was truly enforcing laws that existed instead of broadly analyzing issues associated with cybersecurity. To analyze the existence of these violations, I used the method described in the Methodology section ("GovInfo API"). Some things to note are that legislation has been involved since 1999 regarding data privacy, shown below in Fig. 4. This means that the FTC used an existent norm, so it was doing what was necessary and in its power. Thus, Ruby Corp violated regulatory norms and committed wrongdoing.

Fig. 4: Demonstration of Existence of 1999 Data Privacy Act

Ruby Corp also violated the ethical norm of protecting the data of users. In an interview that Vice held with The Impact Team, the actor responsible for hacking the Ashley Madison site, the hackers were present on the site for "a long time" collecting data and that the security

involved with the web application was “bad,” specifically that one could even use “Pass1234…to VPN to root on all servers.” (Cox, 2015) In cybersecurity, Pass1234 is an example of one of the most common passwords to be used. It is difficult to tell if The Impact Team was exaggerating when it made this claim, as the interview was conducted via email and no tone indicators were given, but it is possible that such simple passwords could have been used without users even being aware of the fact that such little security was used for protecting their data. Additionally, the site’s security must have been so absent if the Impact Team had been present on the site for such a long time. Without information security, there is no data privacy or protection. Thus, the lack of security in the Ashley Madison site means that Ruby Corp violated the ethical norm of protecting users’ data.

As for the Impact Team’s wrongdoings, the Impact Team violated the norm of protecting user’s data. In its statement, the Impact Team mentioned that it started “releasing 2700 transactions,” with full purpose and conviction (Cox, 2015). It next said that everything would be released (Cox, 2015). This includes sensitive and personally identifiable information such as credit card transactions (Cox, 2015). The Impact Team itself seemed unclear as to who it was targeting, because, regardless of users’ intentions, they were most harmed by its actions. Though The Impact Team had no sense of responsibility in protecting users’ data, it still decided to leak information that could have jeopardized many users’ futures, especially economically as one could easily use one of the leaked credit cards. If The Impact Team wanted not to commit wrongdoing, it could have simply ethically hacked the site of Ashley Madison and consulted with Ruby Corp as to how the company could strengthen the security of its website. This action would have protected the data of users. However, The Impact Team chose not to do so and thus committed wrongdoing by violating the ethical norm of protecting Ashley Madison users’ data.

As for the users, they did not commit any wrongdoing by deciding to use the site. The use of the site violated no regulatory or ethical norms. Thus, there was no wrongdoing on the part of the users.

Causal Contribution

For the Ashley Madison data breach of July 2015, causal contribution means performing or failing to perform an action that would have caused the data breach to happen (van de Poel and Royakkers, 2023). Of these two types of actions, Ruby Corp failed to perform actions that eventually led to the breach, and The Impact Team actively performed actions that caused the data breach to occur.

The actions that Ruby Corp failed to perform were also those outlined by the FTC, specifically the action of failing to provide an information security policy, the action of failing to provide reasonable access controls, and the action of failing to provide or enforce system security measures (Staff in the Office of Technology and the Division of Privacy and Identity Protection, 2016). In particular, the need for an information security policy meant that the business could not remain organized around the goal of keeping consumer data safe. The lack of reasonable access controls would make hacking the site easier, as people could easily utilize a highly privileged account through a password-cracking scheme similar to that performed by The Impact Team. This, combined with the ineffective security measures overall, would leave the system vulnerable and sensitive to the actions of The Impact Team. Thus, these actions of wrongdoing, are also classified as actions that would provide a causal contribution to the Ashley Madison data breach of July 2015.

The Impact Team also committed actions of causal contribution, by hacking the site and releasing the private, personal data of the users. Though it did not cause the system's

vulnerabilities, it exploited them to cause harm to users, through exploiting vulnerabilities such as the lack of effective passwords (Cox, 2015). Thus, the Impact Team acted in a way that counts as a causal contribution.

None of the actions the users conducted counted as actions of causal contribution. In using the site, they did not make it more susceptible to weaknesses or vulnerabilities. As a result, the users of Ashley Madison did not causally contribute to the data breach.

Foreseeability

Actors should be able to know the consequences of their actions, as foreseeability entails (van de Poel and Royakkers, 2023). Ruby Corp knew the consequences of its actions and thus met the condition of foreseeability. In particular, according to Ruby Corp, it "ha[s] had stringent security measures in place," and it also mentioned, in an obvious sense, that "these security measures have… not prevented this attack to [its] system." (Macri, 2015) If one already has secure measures in place, one will know the consequences of their actions. Otherwise, the site would have just been left open to invaders like The Impact Team. When a site commits to security measures, it commits to the most secure measures, because all sites truly know the consequences of poor security. Additionally, in a statement by Attorney General Racine in 2016, Ruby Corp "misrepresented the strength of [its] security" in designing, developing, and maintaining Ashley Madison ("Owners of Ashley Madison Enter Into Settlement with District, Other States, and FTC Concerning Data Breach", 2016). In being deceptive about the Ashley Madison site's security, Ruby Corp knew what it was doing as an entity. To say that its security may not be the best is not what any company would do, but to misrepresent the security and make it sound better than it means that one knows the consequences of poor security. Thus, Ruby Corp met the condition of foreseeability.

The Impact Team also met the condition of foreseeability by knowing that its actions would result in consequences. It did not hack the site by accident, it planned the event - as evidenced by the fact that it said that it "worked hard to make [a] fully undetectable attack." (Cox 2015) That would certainly take a long time. Considering that it said it worked hard, some element of purpose was there, and thus, foreseeability. One can predict that something will happen if they put effort into an action.

The users did not know the consequences of using Ashley Madison. As a result, they do not qualify as receiving the condition of foreseeability. In particular, they did not know that using Ashley Madison would result in a data breach, meaning they do not qualify for the foreseeability condition for moral responsibility.

Freedom of Action

Freedom of action means that one must not have had to act under being forced by another entity (van de Poel and Royakkers, 2023). In this case, Ruby Corp exhibited freedom of action. There is no evidence that it was forced by an external entity to have poor security practices because if it was forced to do so, it would have gone public through its statement (Macri, 2015). Additionally, The Impact Team exhibited freedom of action, because the actor was not compelled to hack the site by another entity. No evidence exists that could show that The Impact Team was compelled to hack the site. The users are disqualified from being included because they did not contribute to the Ashley Madison data breach.

As previously stated, the users are disqualified from being included as actors who had freedom of action to qualify for moral responsibility because they did not contribute to the Ashley Madison data breach. One may argue that the Ashley Madison users had freedom of action by not being compelled to use the site with their user-made security measures like having

a strong password, changing their passwords frequently, etc. While it is true that Ashley Madison users are responsible for their level of security, if the level of privacy is so poor that Ruby Corp "can log in and look up transactions", then all of that security is a waste (Cox, 2015). This means that the data itself was not encrypted well enough, for the company itself to be able to look at transactions. Privacy and security are interrelated, privacy can ensure security, and security can ensure privacy, but here, personal methods of security would certainly not be enough for the barrage of poorly encrypted data that The Impact Team released to the public. Thus, the users could not have conceivably contributed, with their poor security measures, to the data breach if the company had such negligent security practices that even with a strong user-involved security the data could have easily become unencrypted and released to the public. Since their actions would have become insignificant in the face of the company, the users are disqualified from having freedom of action concerning the Ashley Madison data breach of July 2015.

Analysis of Responsibility

The analysis of the actions of the primary actors of Ruby Corp, The Impact Team, and Ashley Madison users, against the conditions for responsibility: wrongdoing, causal contribution, foreseeability, and freedom of action, is outlined in Table I:

Conditions for Moral Responsibility				
Company	Wrongdoing	Causal Contribution	Foreseeability	Freedom of Action
Ruby Corp	**Present**	**Present**	**Present**	**Present**
The Impact Team	**Present**	**Present**	**Present**	**Present**
Ashley Madison Users	Absent	Absent	Absent	Absent

Table I: Analysis of Moral Responsibility for Three Primary Actors

As seen in the table, Ruby Corp and The Impact Team are both actors that meet all of the conditions to be considered morally responsible for the Ashley Madison data breach of July 2015. Thus, Ruby Corp and The Impact Team are morally responsible actors. The Ashley Madison users do not meet any of the criteria for being morally responsible users of the site, since they decided to only use the site and were not responsible for the poor security of the site that led to this data breach.

Conclusion

Moral responsibility lies in the hands of Ruby Corp, as an actor and network builder, because it meets all four of the conditions of responsibility - it committed wrongdoing by violating norms, it causally contributed to the breach, it had foreseeability of the consequences, and it exhibited freedom of action. The Impact Team, as an actor, also met all of the four conditions of responsibility, by violating norms, causally contributing to the breach, being able to foresee the consequences, and exhibiting freedom of action. The Ashley Madison users, as an actor, did not meet the conditions of moral responsibility because they did not directly contribute to the actual breach. These were the three primary actors involved in the actor-network analysis as a part of the Ashley Madison network.

The Ashley Madison data breach of July 2015 is essential to analyze in a formalized manner through an ethical framework because this will help the nation understand cybersecurity incidents and the concept of blame and accountability associated with these breaches. This framework-based analysis of the Ashley Madison data breach will also help regulatory entities such as the United States Congress create data privacy legislation that will shift blame away from the users and toward companies responsible for insecure sites and applications and groups

that invade the applications. Since the Ashley Madison case resulted in multiple suicides, knowledge of who to blame and understanding that the users are not at fault will help save lives in the future. Overall, even for sites as controversial, this analysis will shift the narrative from blaming the data breach victims toward holding the company and the hackers responsible, because life is worth so much.

Word Count: 3664

References

Cox, J. (2015, August 21). *Ashley Madison hackers speak out: "nobody was watching."* VICE. https://www.vice.com/en/article/bmjqyz/ashley-madison-hackers-speak-out-nobody-was-watching

Cressman, D. (2009). *A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation*.

Cross, C., Parker, M., & Sansom, D. (2018). Media discourses surrounding 'non-ideal' victims: The case of the ashley madison data breach. *International Review of Victimology*, *25*(1), 53–69. https://doi.org/10.1177/0269758017752410

GovInfo API. (n.d.). https://api.govinfo.gov/docs/

Jones, Sakinah. (2017). Having an affair may shorten your life: the ashley madison suicides. *Georgia State University Law Review, 33(2),* 455-484.

Macri, A. (2015, August 18). *Statement from Avid Life Media Inc. – August 18, 2015*. Ashley Madison Media. https://web.archive.org/web/20150819035058/http://media.ashleymadison.com/statement-from-avid-life-media-inc-august-18-2015/

Owners of Ashley Madison Enter Into Settlement with District, Other States, and FTC

Concerning Data Breach. Newsroom. (2016, December 15). https://oag.dc.gov/release/owners-ashley-madison-enter-settlement-district

Staff in the Office of Technology and The Division of Privacy and Identity Protection. (2016, December 14). *Operators of AshleyMadison.com settle FTC, state charges resulting from 2015 data breach that exposed 36 million users' profile information*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2016/12/operators-ashleymadisonc om-settle-ftc-state-charges-resulting-2015-data-breach-exposed-36-million

van de Poel, I., & Royakkers, L. (2023). *Ethics, technology, and engineering: An introduction*. Wiley-Blackwell.