RISK INNOVATION NEXUS

CASE STUDY

Flo: Women's Health app that tracks personal health information

What happens when a healthcare company shares personal information with a tech giant – without its patients' consent?

THE COMPANY:

Flo is a women's health app that tracks users' hormonal cycles though uploaded data. Flo enables women to take healthcare into their own hands and make informed personal decisions, with many women using the app for pregnancy planning.

WHAT WENT WRONG:

In early 2019, Flo was the top ranked health app in the Apple App Store with a positive reputation for helping women. That changed when the Wall Street Journal published an article about Flo's privacy policies, revealing that the app shared all of their users' information with Facebook. Anytime a user entered information into Flo, the data was immediately sent to Facebook – whether or not the user had a Facebook account[1]. Facebook sold this data to third-parties for targeted consumer ads, resulting in pregnant users seeing ads for baby supplies[2]. Once news broke that Flo was sharing users' health information with a company that would then sell it, users questioned what Flo was doing with their information – especially since the app contained their personal health data. While users had to sign a mandatory privacy agreement, how the app was using the data wasn't clear, frustrating and upsetting users. Users wondered how Flo could be so reckless with such important information and use the data for unauthorized purposes. As the PR nightmare unfolded, Flo struggled to defend their privacy management decisions from questioning by journalists and customers alike[3].

THE CONSEQUENCES:

After the Wall Street Journal article was published, Flo immediately changed their privacy policy and told users that it would "substantially limit" the information shared – likely losing profit gained by sharing data with advertisers. Flo also changed their user agreement and privacy policy on both their app and webpage, stating in more direct terms how user data would be handled. While this was an effective data management decision, for many users it was too late. When users found out about Flo's use of data, their perception of Flo was permanently changed, and many previous users deactivated their accounts. Customers like Alice Berg deleted the app, commenting, "I think it's incredibly dishonest of them that they're just lying to their users especially when it comes to something so sensitive"[1]. While Flo continues to operate today, they continue to lose clients and trust because of a preventable PR nightmare – all because they acted too late. By thinking about how customers would perceive their actions, the company could have prevented the financial loss of ad revenue and the loss of customer trust and loyalty.

LESSONS LEARNED:

Flo threatened critical areas of value with an unclear data management plan. Their enterprise wasn't damaged because they sold personal data, but because customers had a different perception of what the company did with the data. Had they considered users' privacy and perception of their company earlier, analyzing how their use of client data would be perceived, Flo might have been better prepared to address users' privacy concerns. By thinking about orphan risks such as privacy, loss of agency, and perception before the scandal, Flo could have continued to collect data while managing the data in a way that addressed customers' concerns.

Risk Innovation approaches risk as a threat to value, or a threat to something of importance to your enterprise, your investors, your customers, or your community. Whether tangible or intangible, a current product or a future success, if it's worth something to you or your stakeholders, it's an area of value. By identifying what is most valuable in each of these areas, you can begin to more clearly see how and where orphan risks might have the most blindsiding impact.

AREAS OF VALUE:

ENTERPRISE:

+ Improved health and wellbeing of customers

+ Millions of customers who trust and use the app

INVESTORS:

+ Data that can be monetized

+ Regular increase of monthly users

CUSTOMERS:

+ Innovative way to track personal health

+ Real-time personal information database

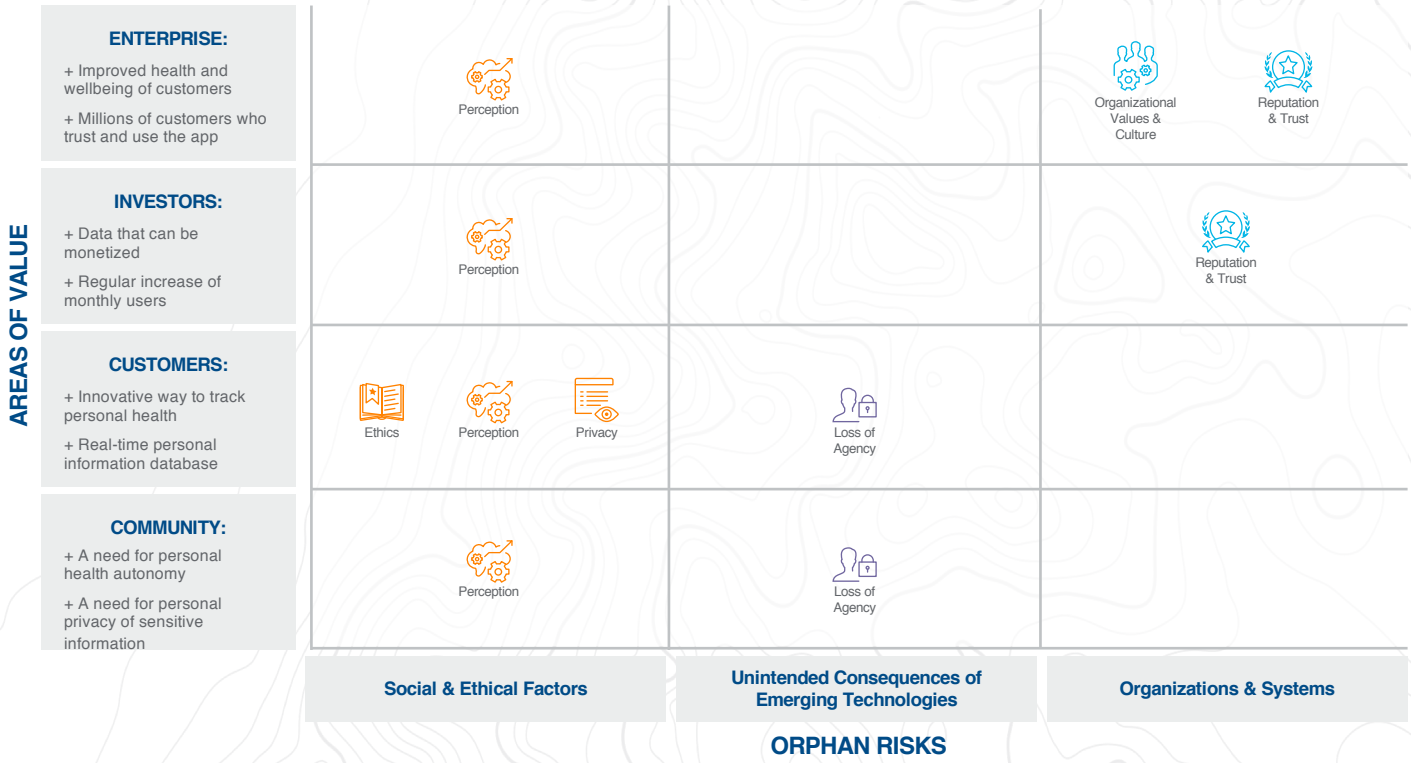
COMMUNITY:

+ A need for personal health autonomy

+ A need for personal privacy of sensitive information

RISK LANDSCAPE:

How did the perception of Flo's data management strategy risk their areas of value?



NAVIGATING THE ORPHAN RISK LANDSCAPE:

A key benefit to mapping out the risk landscape is the ability to see where orphan risks are most concentrated and which risks threaten multiple stakeholders, this allows a company to focus resources and begin planning.

Based on the risk landscape above, Flo could have protected and enhanced value to the company and its stakeholders by:

Focusing on consumer perceptions and ethical practices: By asking questions like "how do we be more transparent about how we use customer data?" and "how do our data decisions affect the trust and loyalty of our customer base?" Flo could have anticipated and put plans in place to avoid the threats that blindsided them. These plans could have been strengthened by considering the primary purposes of data collection, and how they could use data in a way that both helps the company and its customer.

Addressing potential loss of agency: Flo was blindsided by perceived and actual loss of agency amongst its users. This could have been avoided by better-understanding how poor data policies might threaten the autonomy of its customers, and their ability to take control of their lives.

Working harder to build and maintain trust: Where a product like Flo stands or falls on the trust and confidence of users, actions that potentially undermine this can be devastating—even when they make short-term financial sense. In Flo's case, having a greater awareness of threats to reputation and trust, and ways of addressing these, could have helped avoid decisions that ended up blindsiding the company.

This case study is just the beginning of a larger conversation. If you are ready to incorporate risk innovation thinking into your organization, please contact us at info@riskinnovation.org

REFERENCES:

[1] Schechner, S. and M. Secada. (2019, Feb 22). You Give Apps Sensitive Personal Information. Then They Tell Facebook. Retrieved from wsj.com

[2] Kresge, N., I Khrennikov, and D. Ramli. (2019, Jan 24). Period-Tracking Apps Are Monetizing Women's Extremely Personal Data. Retrieved from bloomberg.com

[3] Schechner, S. (2019, Feb 24). Eleven Popular Apps That Shared Data With Facebook. Retrieved from wsj.com

[4] Associated Press. (2019, Feb 22). Facebook Reportedly Received Users' Sensitive Health Data from Apps: "It's Incredibly Dishonest." Retrieved from cbsnews.com