Privacy Risk

The growing concern about the risk of exposure of User Private Information has been labeled as a **Privacy Risk** that has been legislated into a legal and reputation risk for Enterprises that collect and store that information. It is suggested that the NIST Privacy Framework be renamed to the Privacy Risk Framework to more accurately frame the purpose of the documents as it appears for the scope that user concerns are not reflected, expect to the extent they those user concerns impact the enterprise.

Author

Tom Jones (2019-01-04)

Context

User Risk

The meaning of the term Privacy has been growing as the Information Age has expanded into every aspect of our human experience. While it started with the Warren and Brandeis article as the "right to the let alone" [1] it has expanded into a wide range of User Rights. While users have shown increasing anxiety about their privacy, they continue to show very little appetite for changing their behavior to protect their Privacy. As a result federal and state governments around the world have been passing laws designed to give users more control over their User Information.

Enterprise Risk

While in an earlier age it was possible to appeal to an Enterprise's good will, in an age of "maximizing shareholder value" the only way to coerce socially beneficial behaviors from the Enterprise is by demonstrating risks to their continued profitability or existence. There are two broad categories of Enterprise Risk: Legal risk and Conduct Risk.

Legal Risk

- Compliance with legislation mandates always entail additional expenses for a provider hosting user information, both continuing operational costs and fines for non-compliance.
- The risk of tort costs will also expand with additional legislation mandates, both for lawyer’s fees and judgements, especially class action judgements.

Conduct Risk

Since executive compensation is increasingly predicated on shareholder value, any risk must be measured strictly in that metric to become an important consideration for executive action by the bulk of public companies. A similar calculus will apply to public enterprises because of

pressures from the population at large and thanks to the investigations of a free press where it still exists. In both cases Conduct Risk is a growing discipline that Enterprises have learned to fear through the experiences with general business cases describe on the page Conduct Risk as well as those cases that are specific to service providers. For example, since the 2016 US presidential election Facebook has been called on the carpet in several countries for numerous privacy lapses that continue to grow.[2][3] When Facebook reported that 3 million users in Europe had abandoned them it lost $120 Billion in market value and the stock has continued to lose value throughout 2018.[4] The loss to Equifax market cap after their privacy breach is more that 30% with some experts doubting that the company can continue in existence after all the legal cases are settled.[5]

Problems

- Compliance by any Web Site with the agreed terms will be hard to track which means that we can expect to see unanticipated substantial loses as regulatory and market forces exact penalties for unsafe behavior.

Solutions

- It would probably improve the conversation to change the discussion from Privacy to User Rights, but habits and meanings of words are had to change, so it may be necessary to continue to talk about Privacy even though it would be more informative to talk about User Rights.
- Changing corporate habits can be difficult unless the CEO of the Enterprise makes and enforces a commitment to treating customer with respect. [6]
- Large accounting firms have all started "Conduct Risk" practices due to the growing demand, but also to the expectation of continued pressure from regulatory bodies to assure that Enterprises are positioned to absorb the costs of unsafe behavior.
- The best solution would be for financial disclosure documentation to require the inclusion of a conduct risk assessment in every mandated disclosure, with privacy risk as a component of that section. This procedure will never anticipate changes brought about by radically new technologies, but it will require inclusion of risks as them are recognized.
- The most valuable contribution that a privacy risk framework would be to give guidance to accounts performing conduct risk assessment into the areas where ongoing analysis was required.

References

1. Warren and Brandeis *The Right to Privacy* (1890-12-15) Harvard Law Review http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
2. Kevin Roose, *No gentile Giant, But a Juggernaut Playing Hardball.* (2018-12-06) p. B1 New York Times
3. Adam Satariano +1, *Leveraging User Data To Show Favoritism Among Its partners.* (2018-12-06) p. B1 New York Times

4. Over $119bn wiped off Facebook's market cap after growth shock. The Guardian https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock
5. *Equifax's stock has fallen 31% since breach disclosure, erasing $5 billion in market cap.* (2017-09-14) Market Watch https://www.marketwatch.com/story/equifaxs-stock-has-fallen-31-since-breach-disclosure-erasing-5-billion-in-market-cap-2017-09-14
6. Time magazine special report on Habits