Data Breach Reporting Requirements Must Change In AI Age

By **Collin Walke** (July 30, 2024)

Collin Walke

Because artificial intelligence radically reduces the amount of time it takes to sift through data and create relationships between data, it is no longer necessary for nefarious actors to hack personally identifiable information from websites like Ashley Madison, which offered discrete affairs and was hacked in 2015, in order to obtain or infer sensitive details about a person's life.[1]

In the age of AI, the recent hack involving AT&T Inc. and nearly all of its customers' call logs is likely to contain sufficient information from which inferences of affairs or other sensitive information could be made.[2]

This is why regulators — in states and at the federal level — must completely rethink their approach to cybersecurity reporting requirements.

Why AT&T Hack Should Prompt Rethinking Breach Disclosure Requirements

As recently as December 2023, the Federal Communications Commission explained that

> telecommunications carriers ... often collect large quantities of sensitive customer data. Information such as records of the telephone numbers a person has called, or mobile phone location data showing the places they have been, can provide insights into medical conditions, religious beliefs, personal associations, and many other aspects of an individual's private life.[3]

However, the FCC adopted a four-factor, harm-based trigger analysis before applicable companies are required to notify consumers. The four factors to be considered are:

1. The sensitivity of information, in totality, that was the subject of the breach;
2. The nature and duration of the breach;
3. Mitigations; and
4. Intentionality.[4]

Hypothetically, would the hack announced by AT&T on July 12 fall under the harm-based trigger? The sensitivity of information, especially given AI, seems to weigh heavily in favor of reporting.

But, the duration of the breach is relatively limited, and AT&T acted quickly and in coordination with law enforcement such that it appears an individual has been apprehended and the hacked information is not currently publicly available.[5]

Thus, these two factors appear to weigh against disclosure. The intentionality factor appears to weigh in favor of disclosure. So, a good faith argument could be made that there's a 50/50 decision in this scenario to report. Given the FCC's concerns of underreporting breaches,[6] is the harm-based trigger analysis sufficiently clear?[7]

Comparatively, the U.S. Securities and Exchange Commission's Form 8-K filings look to protect investors, not consumers. Form 8-K requires applicable companies to detail any material impact on operations or financial condition of the company following a breach. [8]

As a result, in spite of the fact that nearly every single AT&T customer's call-log information was hacked and is susceptible to AI inferences, investors should arguably not be concerned because, according to AT&T, the hack has not had an impact on operations or financial condition.[9]

If the hack does not have an impact on operations or the financial condition of AT&T, that does not necessarily speak harm to any particular set of the hacked customers, who might in fact experience negative impacts.

The FCC adopted the harm-based trigger analysis because the majority of state-level reporting requirements are premised upon similar concepts.[10] But, even when adopting a harm-based analysis, state-level definitions of harm can be far weaker.

For example, Oklahoma's breach reporting requirement is far narrower than the FCC's, and likely, would not have required AT&T to report the breach, if it were otherwise applicable.[11]

There are obviously a myriad of other breach reporting laws on the books, like the Health Insurance Portability and Accountability Act,[12] but they all fail to account for what's coming and fail to account for what currently exists.

That is why, to this day, there is litigation as to whether individuals possess standing to bring lawsuits for a mere breach of their data, or, must prove actual damages as a result of the breach.[13] Regulators could have done more to clarify this and will have to do so in the future in order to protect consumers.

To add to the reporting hurdles, there are often law enforcement carveouts that permit delays in reporting under certain circumstances, such as when disclosure would aid in the capture of the bad actors or would serve national security interests.[14]

Obviously, given the inherent illegality of any hack, these narrow delays are important, but how much discretion is afforded is industry- and jurisdiction-specific, depriving consumers of uniformity in knowing about potential disclosures of their information.[15]

Every expert agrees that the impact AI will have on society will be exponential. Meaning, the time it will take for a hacker to appropriate and then misuse data will exponentially decrease with AI.

This means that disclosures relating to breaches in the future will have to be quicker because bad actors will be able to exploit consumers with misappropriated data sooner than has historically been true.

Antiquated Concepts

AI's ability to determine relationships coupled with generative AI's improvements in deepfake technology means that the very definitions used in so many breach reporting laws need to change.

It used to be that personally identifiable information was generally anything that was linked to or linkable to a person.[16]

But, today, there is almost nothing that wouldn't fall into this category. With data so granular, companies can target you whether your phone is in your pocket or plugged into your headphones, or you're ordering from McDonald's, which recorded customers' voice information when ordering.[17] Almost everything we do is susceptible to analysis and linkage.

Data privacy laws, which work in tandem with cybersecurity laws by minimizing the data available for exploitation, also often draw a now-antiquated dividing line between personally identifiable information and sensitive information,[18] with sensitive information being deserving of greater protections.

Per the FCC and common AI-industry knowledge,[19] even innocuous data points can serve to divulge sensitive personal information. Therefore, a demarcation between personally identifiable information and sensitive data should be disposed of, and all personal data should be treated as though it were sensitive data.

Otherwise, the very harms sought to be prevented by demarcating personally identifiable information and sensitive data will be meaningless in the age of AI.

Regulatory Solutions

As noted by the FCC, cybersecurity reporting requirements are usually mirrored from preexisting legislation.

From a regulatory standpoint, this makes sense because entities sought to be regulated have the ability to comply seamlessly, i.e., compliance with one law likely makes the entity compliant with another.

The problem, however, is that we are living in a fundamentally different threat landscape as a result of AI. Just as courts are struggling with how to determine copyright issues arising from scraped data residing in AI training sets, without adequate guidance, courts and consumers will struggle with how to determine privacy and liability violations arising out of hacks.

The first goal regulators should look to fulfill is adequate legislation, especially in light of the U.S. Supreme Court decision in Loper Bright Enterprises v. Raimondo,[20] which did away with the Chevron deference standard.

Adequate legislation should obviously consider industry-specific nuances, but, practically, is there a fundamental difference between a consumer's data coming from call logs, Ashley Madison, or a medical provider if the same embarrassing or compromising inferences can be made?

Further, adequate legislation should address a consumer's right to a private right of action and standing in the event of a breach.

There are a litany of arguments for or against a private right of action; however, absent a private right of action, adequate legislation must ensure adequate funding for agencies to prosecute and pursue violators on behalf of consumers. Otherwise, the legislation would be devoid of any real teeth.

The second goal regulators should look to fulfill is timeliness of disclosures. A recent analysis from the International Association of Privacy Professionals concluded:

> Predictive AI could integrate business continuity and disaster recovery plans, which generative AI could likely help appropriate professionals create, with incident response plans to suggest next courses of action during remediation of a breach. Generative AI could create breach-notification letters, and, when the dust settles, predictive AI could use the information collected in the response to generate suggested security and privacy practice enhancements.[21]

This means that companies should be required to adopt AI and machine learning technologies that expedite notifications to customers. Congress has previously strongly encouraged the adoption of technology in industry-specific situations.[22] Moreover, written notifications to consumers should be reconsidered in light of the ubiquity of e-communications.

After all, if consumers can receive a text reminder to pay their bill, then companies should be capable of texting consumers following a hack or provide similar e-communications, especially with the development of AI and machine learning notification systems.

The triggering event for consumer disclosures should not be limited to a harm-based analysis since it is impractical to determine its applicability, especially when AI can take innocuous data and infer nocuous characteristics.

All data is now sensitive when hacked, and therefore, is always harmful when hacked. To address this problem, the triggering event for consumer disclosures should be anytime a consumers' data is hacked. Period.

The third and final goal of regulators should be to ensure that all consumer data is encrypted to the maximum extent feasible. As of now, the FCC has an encryption safe harbor, where hacked encrypted data that is not at risk of decryption is not required to be reported to consumers.[23]

However, the use of encryption is optional under FCC reporting requirements.[24] Consumers are not protected by making encryption optional. Therefore, regulators should mandate encryption.

Technological advances always call for the development of new regulations. The problem, however, is that regulators are building upon antiquated frameworks. The frameworks themselves need to be reconsidered just as every other aspect of our lives is being reconsidered in light of AI development.

Failure to act now will not only increase technical debt for companies,[25] but it will also increase the odds that consumers will be exploited.[26] In fact, a recent poll by Reinsurance News of the insurance and reinsurance industry found that "nearly half of respondents (45%) said that they expect AI-powered threats to be the biggest driver of losses over the next two years."[27]

Regulators, consumers and businesses cannot wait any longer for meaningful changes to data breach reporting requirements. The future is here, and it is time to act.

Collin R. Walke is a shareholder and leads the cybersecurity and data privacy practice group team at Hall Estill.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See: "A Retrospective on the 2015 Ashley Madison Breach," https://krebsonsecurity.com/2022/07/a-retrospective-on-the-2015-ashley-madison-breach/ (last visited 7/18/2024).

[2] See: "AT&T says hackers stole records of nearly all cellular customers' calls and texts," https://www.nbcnews.com/news/us-news/t-says-hackers-stole-records-nearly-cell-customers-calls-texts-rcna161507 (last visited 7/18/2024).

[3] See: Federal Communications Commission December 13, 2023 Report and Order, https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf, at p. 2 (last visited 7/13/2024).

[4] See: Id., at pp. 34-5.

[5] See: "AT&T says hackers accessed records of calls and texts for nearly all its cellular customers," https://www.cbsnews.com/news/at-t-data-breach-records-calls-texts-was-i-affected/#:~:text=While%20the%20files%20don't,AT%26T%20said%20in%20the%20statement (last visited 7/18/2024).

[6] See: n. 4, at pg. 14.

[7] Perhaps in this case, given the shear size of the breach, and resulting potential PR pitfalls, a company would voluntarily choose to disclose to prevent further damage to reputation.

[8] See: SEC Form 8-K, at pg. 11; https://www.sec.gov/files/form8-k.pdf (last visited 7/18/2024).

[9] See: July 23, 2024, AT&T 8-K filing; https://otp.tools.investis.com/clients/us/atnt2/sec/sec-show.aspx?Type=html&FilingId=17677638&CIK=0000732717&Index=10000 (last visited 7/13/2024).

[10] See: n. 3, supra, at p. 31.

[11] See: Okla. Stat. tit. 24, § 162(1) (requiring threat of disclosure in order to report, and AT&T does not believe the hacked information has been made available to the public).

[12] See e.g., C.F.R. § 164.408.

[13] See e.g., Maendele v. North Oklahoma County Mental Health Center, Inc., Case No. 120,862 (Oklahoma Court of Civil Appeals) (unpublished opinion) at pp. 4-5 (discussing federal circuit split on Article III standing).

[14] See e.g., n. 3, supra, at n. 26.

[15] Cf. HIPAA reporting requirements at 45 C.F.R. § 164.408(c)(less than 500 individuals, report may be made as late as 60 days after the end of the calendar year) and SEC Final

Rule at p. 44 (declining to include an individual threshold)(https://www.sec.gov/files/rules/final/2023/33-11216.pdf) (last visited 7/18/2024).

[16] See generally, U.S. Department of Labor, Guidance on the Protection of Personal Identifiable Information, https://www.dol.gov/general/ppii (last visited 7/18/2024).

[17] See: "McDonald's Takes Voiceprints During Drive-Thru Trips, Alleges Class Action Lawsuit," https://topclassactions.com/private/mcdonalds-takes-voiceprints-during-drive-thru-trips-alleges-class-action-lawsuit/ (last visited 7/18/2024).

[18] See e.g., Colorado Privacy Act, 6-1-1303(24) (defining "Sensitive Data").

[19] See "How Target Figured Out a Teen Girl was Pregnant Before Her Father Did," https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ (last visited 7/18/2024) (explaining innocuous details leading to the determination of pregnancy).

[20] 144 S.Ct. 2244 (2024).

[21] See: "Evaluating the Use of AI in privacy program operations," Byrant, J.S., https://iapp.org/news/a/evaluating-the-use-of-ai-in-privacy-program-operations (last visited 7/30/2024).

[22] See e.g., 42 U.S.C.A. § 300jj-11 et seq.

[23] See: n. 3, supra, at p.35.

[24] Id.

[25] "Technical debt" "eventually cause the software to deviate from its prescribed nonfunctional requirements, and in the long-term, they can impact performance, scalability, resilience or similar characteristics of the system." Gartner, Technical Debt, https://www.gartner.com/en/information-technology/glossary/technical-debt (last visited 7/18/2024).

[26] n. 21, supra.

[27] Reinsurance News, "Poll suggests AI threats will drive the biggest cyber losses for re/insurers," https://www.reinsurancene.ws/poll-suggests-ai-threats-will-drive-the-biggest-cyber-losses-for-re-insurers/#:~:text=Of%20this%2C%20nearly%20half%20of,the%20sector%20in%20recent%20years (last visited 7/18/2024).