

Before the
FEDERAL COMMUNICATIONS
COMMISSION
Washington, DC 20554

In the Matter of Data Breach Reporting Requirements	WC Docket No. 22-21
--	---------------------

In the Matter of)	
)	
Data Breach Reporting Requirements)	WC Docket No. 22-21
)	

REPLY COMMENTS OF JUST FUTURES LAW

Julie Mao
Just Futures Law
95 Washington St., Suite 104-149
Canton, MA 02021

Laura M. Moy
Daniel Jellins
Institute for Public Representation
Georgetown University Law
Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9535

Electronically Submitted March 24, 2023

Table of Contents

Table of Contents	2
I. INTRODUCTION AND SUMMARY	2
II. CONSUMER INTERESTS OF CONTROL AND PROTECTION OF THEIR DATA ARE BEST SERVED THROUGH A NO-TRIGGER BREACH NOTIFICATION REGIME WITH APPROPRIATE INFORMATION REGARDING THE BREACH.	4
III. NO TRIGGER REGIMES ENCAPSULATE A WIDE VARIETY OF HARMS THAT WOULD BE OVERLOOKED BY A HARM TRIGGER	6
IV. IF A HARM-BASED TRIGGER IS IMPLEMENTED, THE COMMISSION MUST EXPAND THE DEFINITION OF BREACH AND HARM.	8
V. CONCLUSION	9

I. INTRODUCTION AND SUMMARY

Data breaches have become more prominent in today's landscape and are affecting consumers to a greater degree in various forms of harm. Just Futures Law (JFL) is a transformational immigration lawyering organization that provides legal support for grassroots organizations engaged in making critical interventions in the United States' deportation and detention systems and policies. JFL staff maintain close relationships with organizations and activists who seek to understand the scope and range of government surveillance and criminalization. The organization's staff have decades of experience in providing expert legal advice, written legal resources, and training for immigration attorneys and criminal defense attorneys on the immigration consequences of the criminal legal system. JFL has a significant interest in the administration of government surveillance and data collection. Just Futures Law files this reply comment to speak to one important issue in the above-captioned docket: We urge the FCC not to adopt a harm-based trigger for breach notification, under which telecommunications providers would only have to notify their customers of a data breach after performing an analysis and determining that some form of legally cognizable harm to consumers would be likely to occur as a result of the breach.

Under the current data breach notification regime, service providers notify consumers whenever a data breach occurs. Data breach notifications allow consumers to react to breaches by taking steps to reduce any harm that arises. A proposed harm trigger rule would not benefit consumers and would instead put consumers at more risk for harm for several reasons.

First, a proposed harm trigger rule would deprive consumers of choice in dealing with potential data breach fallout. After receiving a breach notification with appropriate

information consumers can assess the situation and determine if further action is warranted. Consumers can capably engage in risk analysis after receiving a breach notification. After all, the data belongs to consumers, who deserve a choice in overseeing remediation steps taken if necessary. Providers should not be in charge of deciding whether there is sufficient likelihood of harm after a data breach to notify consumers. Namely, providers don't have the most substantial incentive to notify consumers after suffering a data breach. And despite arguments to the contrary, commenters have yet to provide evidence that the current regime burdens consumers with fatigue notification. Such an argument relies on the premise that consumers cannot digest data breach notifications and perform a risk analysis. This premise is flawed and incorrect.

Second, a proposed harm trigger rule will not produce the benefits to consumers touted by providers or increase data security. Data breach notifications serve to increase public awareness of data breach dangers. Additionally, data breach notifications keep providers honest by compelling them to disclose whenever a data breach occurs. In a proposed harm trigger regime, fewer notifications based on a harm threshold impose less reputational pressure on providers. Despite provider claims, less reputational pressure will not lead to increased investment in cybersecurity measures. Consumers have options in the provider marketplace, and data security is an essential part of their choice. Data breach notifications are integral to determining the cybersecurity strength when choosing a provider. A harm trigger would likely result in lesser or stagnant cybersecurity practices or measures due to fewer consumer notifications. In this scenario, consumers suffer as the market has less incentive to

innovate. Also, it is more difficult for consumers to differentiate providers based on data security and control.

Lastly, consumers are best served under the current no harm trigger regime, which ensures that consumers receive a notification regardless of the type of harm that could ensue—including harms experienced only by a minority of consumers, and those that are not recognized under all legal regimes. Commenters have mainly advocated for a harm trigger that concentrates on financial harm. However, consumers potentially suffer various harms from data breaches beyond economic harms. Data breaches can cause physical, emotional, and reputational harm. These harms are concrete and actual and not theoretical, as some commenters claim. The current no trigger regime allows consumers to examine every data breach for these harms, which a harm trigger would ignore.

We urge the Commission to protect consumers by not implementing the proposed harm trigger rule. Alternatively, if a harm trigger rule is implemented, the Commission should adopt expansive definitions of harm and breach so that consumers receive notifications about unauthorized access to or use of their information in as many cases as possible. An expansive definition of harm would conform to the word's plain meaning and its ordinary usage and would encompass situations in which some people might reasonably be concerned about possible harm, such as when providers share information with law enforcement representatives or impostors without a lawful order and without following appropriate process. Additionally, defining harm in an expansive manner would avoid confusing consumers about the potential harm data breaches can produce. Moreover, a broad harm definition would prevent superfluity and

inconsistency in the rule by fully encompassing all consumer harm. Lastly, an expanded breach definition would mirror the landscape of growing data breaches that extend beyond intentional access. Even when data breaches are inadvertent, the consumer can still suffer a range of harm. Only by expanding the definition of harm and breach will a harm trigger adequately protect consumers from danger.

II. CONSUMER INTERESTS OF CONTROL AND PROTECTION OF THEIR DATA ARE BEST SERVED THROUGH A NO-TRIGGER BREACH NOTIFICATION REGIME WITH APPROPRIATE INFORMATION REGARDING THE BREACH.

Consumers, not providers, should decide whether they could be harmed by a breach of their customer proprietary network information (CPNI) because the data belongs to consumers. Consumers should be in control. Consumers can already properly analyze a data breach harm. The proposed rule would give an unjustified amount of deference to companies. In contrast, the current no-trigger rules generates greater consumer awareness of the dangers of data breaches.

Given the proper information, consumers themselves are best situated to analyze the potential harms and decide the necessary next steps of a breach of their data. If adopted, the proposed rule would take away consumer control of deciding what necessary next steps to take. The proposed rule would transfer to companies the authority to decide whether consumers are likely to be harmed by such a breach. Customers, not companies, should be the ones to decide what to do after a breach of their information.

To facilitate consumers' ability to analyze their own risk of harm and take steps to protect themselves accordingly, the Commission should not only maintain the no-trigger standard, but also specify the minimum information that must be included in a

notification. Currently, the rules specify when and to whom breach notifications must be made, but do not address the content of such notifications.¹ Including general information about how the breach occurred resolves the issue of when an employee of a provider accidentally receives access to CPNI but does not misuse the information.²

With the appropriate notification content, consumers would be able to gauge how best to react to any data breach. For example, if notified about an incident in which an employee of a provider accidentally received access to CPNI but quickly recognized the error and was highly unlikely to misuse the information, average consumers would likely not be alarmed. If given these facts, consumers would not spend “unnecessary time and money to protect their information based on a harmless breach” as some commentators suggest, since it was not caused by malicious intent.³ And importantly, extremely risk averse consumers would still be able to spend time and money on more protective measures. A no-trigger notification with additional content protects the average consumer and allows for more risk averse consumers to further act.

In particular, JFL urges the FCC to consider the interests of historically disadvantaged and oversurveilled communities, including immigrant and mixed status communities. It is of critical importance that people in these communities have the power to tailor their responses to data breaches to take into account the particular ways in which breaches may affect them differently. For example, when law enforcement receives the CPNI data of people in oversurveilled communities, the potential harm

¹ See 47 CFR § 64.2011.

² Comments of Sorenson Communications LLC, *Data Breach Reporting Requirements*, Dkt. 22-21, at 1 (filed Feb. 22, 2023).

³ Comments of Verizon Communications Inc., *Data Breach Reporting Requirements*, Dkt. 22-21, at 10-11 (filed Feb. 22, 2023).

transforms from a financial harm into the likelihood of harassment and monitoring. This can materially change the way that people live.⁴

Contrary to some industry commenters' assertions, depriving customers of some of the details of a breach would not serve customers. Specifically, Verizon argues that because it communicates with its prepaid customers about breaches using SMS messaging, which has a 160 character limit, it cannot include all relevant details.⁵ However, as Verizon itself notes, such SMS messaging can include a general description of the breach and links that direct customers to another source containing more information.⁶ Therefore, providers can continue using their methods to contact customers while also being able to include certain information relating to the breach. These are not incompatible.

Relatedly, the current incentive structure for notifying consumers of a breach favors maintaining the no-trigger notification regime. When companies decide what breaches rise to the likelihood of harm threshold, their financial and reputational incentives position them to err on the side of not harmful and non-disclosure. This would have the effect of taking away control from consumers. As Verizon has claimed, customer privacy is a *strategic* priority.⁷ But under a harm trigger regime, companies would value this "*strategic priority*" less. Companies would not be pressured to value customer privacy because they would not have to notify customers of a breach unless

⁴ McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. TIMES (Oct. 2, 2019), <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>.

⁵ Comments of Verizon Communications Inc., *Data Breach Reporting Requirements*, Dkt. 22-21, at 7 (filed Feb. 22, 2023).

⁶ *Id.*

⁷ Comments of Verizon Communications Inc., *Data Breach Reporting Requirements*, Dkt. 22-21, at 3 (filed Feb. 22, 2023).

they decided it met their harm threshold. As such, the proposed rule would under-protect customers, take away consumer control over their own data, and unjustifiably increase company deference.

Erring on the side of more, rather than fewer, breach notifications also benefits the public by raising awareness of data breach harms, ultimately forcing companies to improve their data protection services. Data breach notifications educate people to the dangers lurking in the cybershadows and consumers' vulnerabilities to identity thieves. This greater awareness of breaches would push consumers to demand companies to spend more resources on protecting consumers' data. Companies better able to protect consumer data will supplant those in the market who falter. Thus, more data breach notifications improve the data protection market as a whole because they incentivize companies to make consumer protection a priority.

III. NO TRIGGER REGIMES ENCAPSULATE A WIDE VARIETY OF HARMS THAT WOULD BE OVERLOOKED BY A HARM TRIGGER

The Commission best protects consumers under the current no harm trigger regime, in which providers notify customers of data breaches. The proposed harm trigger rule focuses mainly on financial harms and, if adopted, would preclude consumers from taking preventative protective actions to avoid other types of harm. These harms include physical, emotional, and reputational harms, many of which may fall disproportionately on historically disadvantaged communities. Furthermore, there exist doubts, even from industry representatives, about the success and effectiveness

of harm triggers in enhancing security.⁸ Therefore, the Commission should not adopt a harm-based trigger to protect consumers, especially one that narrowly specifies harm.

Physical and emotional harm can occur from data breaches especially when law enforcement agencies use exposed data. For instance, the exposure of phone location data could result in the physical and emotional harms of incarceration, detention, and deportation. Law enforcement agencies may access exposed location data to decipher home addresses for deportation proceedings. Additionally, correctional officers can abuse location sharing to invasively surveil those in the carceral system and their friends and families.⁹ Friends and family members who communicate with an incarcerated individual are subsequently subject to unlawful monitoring and surveillance by law enforcement.¹⁰ Also, law enforcement can use location data to harass and intimidate activists and historically overpoliced and over surveilled groups.¹¹ Importantly, potential abuses are likely to negatively and disproportionately affect people in disadvantaged and marginalized communities who often lack the necessary resources to assert their rights.¹² The potential abuses of exposed data abound.¹³

⁸ Comments of Lincoln Network, *Data Breach Reporting Requirements*, Dkt. 22-21, at 2 (filed Feb. 22, 2023).

⁹ Comments of Georgetown Law Center on Privacy & Technology, New America's Open Technology Institute, and Free Press, *Unauthorized Disclosure and Sale of Customer Location Information by Wireless Carriers*, at 16 (filed June 14, 2019).

¹⁰ See *id* at 16-17.

¹¹ Natalie Delgadillo, *A Prominent Black Lives Matter Leader is Suing D.C. Police to Prove She's Been Under Surveillance*, DCIST (Feb. 11, 2019), <https://dcist.com/story/19/02/11/this-black-lives-matter-leader-is-suing-d-c-police-for-documents-to-prove-shes-been-under-surveillance/>; See Comments of The Council on American-Islamic Relations, *Request for Investigation of Alleged Violations of Section 5 of the FTC Act by Multiple Actors in the Location Data Industry*, (filed Apr. 12, 2022).

¹² Comments of Georgetown Law Center on Privacy & Technology, New America's Open Technology Institute, and Free Press, *Unauthorized Disclosure and Sale of Customer Location Information by Wireless Carriers*, at 16 (filed June 14, 2019).

¹³ *Id.*

Furthermore, location data exposure can lead to extreme physical harms such as grave bodily injury or death.¹⁴ Bad actors and hate groups can use location data to stalk, harass, threaten, and assault vulnerable groups such as immigrants and domestic abuse survivors.¹⁵ Additionally, bad actors and hate groups can utilize location data to coordinate doxing campaigns against immigrants and other vulnerable groups.¹⁶ Bad actors can also use location data to engage in systematic and repeated surveillance to assert control over targeted groups and individuals.¹⁷ For example, bad actors can use location data to decipher when a house is empty or record an individual's route during the day.¹⁸ Alarming, bad actors can readily obtain location data for a few hundred dollars.¹⁹ Because bad actors can follow and harm targets easily, data breaches and their potential for physical harm can disproportionately affect vulnerable groups.²⁰

¹⁴ Joseph Cox, *Black Market T-Mobile Location Data Tied to Spot of a Triple Murder*, VICE (June 26, 2019, 9:47 AM), <https://www.vice.com/en/article/vb9nzx/black-market-tmobile-phone-location-data-bounty-hunter-murder>.

¹⁵ Comments of Georgetown Law Center on Privacy & Technology, New America's Open Technology Institute, and Free Press, *Unauthorized Disclosure and Sale of Customer Location Information by Wireless Carriers*, at 15 (filed June 14, 2019).

¹⁶ Freddy Cruz, *White Nationalists, Jan. 6 Protesters and Qanon: What You Need to Know About Border Vigilantes Along the Border*, SOUTHERN POVERTY LAW CENTER (Dec. 2, 2021), <https://www.splcenter.org/hatewatch/2021/12/02/white-nationalists-jan-6-protesters-and-qanon-what-you-need-know-about-border-vigilantes>.

¹⁷ *Id.*

¹⁸ Joseph Cox, *I gave a Bounty hunter \$300. Then he Located Our Phone*, VICE (Jan. 8, 2019, 12:08 PM), <https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile>.

¹⁹ Joseph Cox, *I gave a Bounty hunter \$300. Then he Located Our Phone*, VICE (Jan. 8, 2019, 12:08 PM), <https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile>; Joseph Cox, *Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years*, VICE (Feb. 6, 2019, 5:10 PM), <https://www.vice.com/en/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years>; Geoffrey Starks, *Why It's So Easy for a Bounty Hunter to Find You*, N.Y. TIMES (Apr. 2, 2019), <https://www.nytimes.com/2019/04/02/opinion/fcc-wireless-regulation.html>.

²⁰ *Id.*

Larger than just vulnerable groups, the universe of potential physical harm victims means the Commission should interpret the definition of harm to include this kind of harm when assessing a proposed harm trigger rule.

Emotional and reputational harm can also flow from data breaches. Law enforcement agencies have used exposed location data to track citizens without warrants, violating their constitutional rights.²¹ There are serious emotional harms to individuals and their loved ones when people are detained, incarcerated, or deported based on this data. So not only the physical harm, but emotional and reputational harms also arise. Further, reputational and emotional harm can occur when exposed location data is used by law enforcement to obtain evidence illegally, and cases are taken to trial based on that evidence. Individuals and their families can suffer embarrassment and reduced social status from the publicity a trial generates, along with turmoil and uncertainty as the threat of incarceration looms.²² Emotional and reputational harm exist as concrete harms from data breaches that the Commission must not ignore.

IV. IF A HARM-BASED TRIGGER IS IMPLEMENTED, THE COMMISSION MUST EXPAND THE DEFINITION OF BREACH AND HARM.

For the reasons outlined above, JFL strongly urges the Commission to maintain the no-trigger standard for breach notification. However, in the event the Commission

²¹ Doyle Murphy, *Ex-Missouri Sheriff Cory Hutcheson Sentenced to 6 Months in Prison*, Riverfront Times (Apr. 29, 2019, 1:09 PM), <https://www.riverfronttimes.com/news/ex-missouri-sheriff-cory-hutcheson-sentenced-to-6-months-in-prison-31510901>; Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, N.Y. TIMES (May 10, 2018), <https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>.

²² See *Id.*

nevertheless decides to adopt a harm-based trigger, the Commission should broadly construe the definitions of harm and breach. As illustrated above, there are many potential harms that consumers may face as a result of a breach— especially consumers in historically disadvantaged communities. Also, expanding the definition of breach would align with industry trade associations that favor expanding both breach and harm definitions.²³ And while certain industry players only support adding physical harm and inadvertent breaches to both definitions, more is needed to protect consumers sufficiently.²⁴ We urge the Commission to recognize all the myriad and consequential types of harms that exist.

On principle, confining harm to only financial harm would defy the word's plain meaning. The Britannica Dictionary defines “harm” as “physical or mental damage or injury [or] something that causes someone or something to be hurt, broken, made less valuable or successful.”²⁵ A narrow construction contradicts the word's ordinary usage. Common sense dictates that a typical consumer would group other enumerated harms beyond financial harm when using or defining the word “harm.”

Further, limiting the definition of harm to a subset of its usual meaning would render the word insignificant or superfluous. And traditional principles of statutory construction instruct that a statute or rule should avoid superfluity and

²³ Comments of NCTA, *Data Breach Reporting Requirements*, Dkt. 22-21, at 2, 4, 5 (filed Feb. 22, 2023).

²⁴ *Id.*

²⁵ *Harm*, BRITANICA.COM, <https://www.britannica.com/dictionary/harm#:~:text=1%20harm-,%2F'h%C9%91%2F,less%20valuable%20or%20successful%2C%20etc.> (last visited Feb. 20, 2023).

insignificance when possible.²⁶ Diluting the definition of harm would lessen the protection consumers receive. Also, consumers accustomed to the whole meaning of harm could be confused. Consumers would wonder why a notification did not warn them before they suffered harm. As described above, consumers correlate harm with harm beyond financial harm, but a harm trigger would ignore those harms. Consumers would not feel protected by a harm trigger that avoids the swath of harms they suffer, and the word harm in a harm trigger regime would be meaningless. Thus, the Commission should define harm according to its ordinary meaning to avoid superfluity, confusion, and clarify any proposed rule. Physical, emotional, and reputational harm should be incorporated when defining harm to safeguard consumers.

Lastly, to fulfill the NPRM's purpose of protecting consumers, the Commission should interpret "breach" broadly to include inadvertent access. Potential harms exist whenever a data breach occurs, whether intentional or inadvertent. At the very least, the consumer loses control over breached data. However, due to the growing ease with which even seemingly sterile or anonymous datasets can be linked to individuals, breaches may often carry potential for greater harm.²⁷ Previous studies and petitions before the Commission demonstrate this widely known risk.²⁸ Accordingly, the Commission should include inadvertent access in the definition of breach.

²⁶ *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) (stating that it is "a cardinal principle of statutory construction that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.'").

²⁷ Comments of Public Knowledge, *Petition for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers without Customers' Consent Violates Section 222 of the Communications Act*, Dkt. 13-306, at 6-7 (filed Dec. 11, 2013).

²⁸ *Id.*

V. CONCLUSION

We appreciate the Commission's attention to the ever-growing data breach problem and associated harms, and we value the opportunity to comment on data breach notifications. As data breaches grow exponentially²⁹, the associated harms have become increasingly troublesome for consumers³⁰, and it is critical that the Commission shield consumers from these harms. The current no-trigger regime best serves consumers as data breach notifications allow consumers to respond promptly to the harms that arise from data breaches. Such harms include financial, physical, emotional, and reputational harm. These harms are actual and concrete, with potentially grave consequences for consumers. The proposed harm trigger rule would ignore harms other than financial harms and would not benefit consumers. To best safeguard consumers, we urge the Commission not to adopt a harm-based notification trigger. However, if a harm trigger is adopted, the Commission should define harm and breach broadly to mirror the harms consumers face.

²⁹ Bree Fowler, *Data Breaches Break Record in 2021*, CNET (Jan. 24, 2022), <https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/>; Aaron Drapkin, *Data Breaches That Have Happened in 2022 and 2023 So Far*, TECH.CO (Mar. 13, 2023), <https://tech.co/news/data-breaches-updated-list>; *51 Million Americans Were Affected by Healthcare Data Breaches in 2022 Due to Weak Security*, BUSINESSWIRE (Mar. 21, 2023), <https://www.businesswire.com/news/home/20230321005710/en/>; Christian Wiens, *Top Data Breaches in 2022 and 2023 Point to Increases in Phishing and Ransomware*, Security Boulevard (Mar. 23, 2023), <https://securityboulevard.com/2023/03/top-data-breaches-in-2022-and-2023-point-to-increases-in-phishing-and-ransomware/>; Carly Page & Zach Whittaker, *It's all in the (lack of) details: 2022's badly handled data breaches*, TECHCRUNCH (Dec. 27, 2022), <https://techcrunch.com/2022/12/27/badly-handled-data-breaches-2022/>; Comments of Electronic Privacy Information Center, *Data Breach Reporting Requirements*, Dkt. 22-21, at 13 (filed Feb. 22, 2023).

³⁰ *Id.*

Dated March 24, 2023

/s/

Laura M. Moy

Daniel Jellins

Institute for Public Representation

Georgetown University Law Center

600 New Jersey Avenue NW

Washington, DC 20001

Tel. (202) 662-9535

*Kavisha Patel and Joshua Perez, Student Attorneys, Provided Substantial Assistance