October 20, 2021

The Honorable C.E. "Cliff" Hayes, Jr., Chair
Joint Commission on Technology and Science, Consumer Data Protection Work Group
Virginia General Assembly
Richmond, VA 23129

Dear Chair Hayes,

The undersigned groups sincerely thank you for your work to advance consumer privacy in Virginia through the Consumer Data Protection Act (CDPA), which extends to Virginia consumers the right to access, delete, and stop the sale of their personal data, with additional rights for sensitive information. In keeping with the consumer protection intent of the legislation, we recommend that you deny the CDPA carveouts proposed by data brokers RELX and the National Insurance Crime Bureau (NICB) at the August 2021 working group meeting. Neither of these requests is necessary, and both would be harmful to consumer privacy.

RELX requested to amend the CDPA so that data brokers—entities that collect and purchase consumer data from entities other than the consumer itself—may treat deletion requests as an opt out of sale out of concerns that they could not comply with deletion requirements. However, as an active member of the Privacy Shield agreement,[1] RELX has self-certified that they are able to comply with its provisions, which include providing consumers with access to the information held about them, and the ability to delete that information when it is inaccurate or processed in violation of the Privacy Shield principles.[2] Now that the courts have declared the Privacy Shield inadequate,[3] businesses like RELX that process and transfer Europeans' data to the United States

[1] Privacy Shield Framework, "RELX," https://www.privacyshield.gov/participant?id=a2zt0000000KzUvAAK.
[2] Privacy Shield Framework, "Access," https://www.privacyshield.gov/article?id=8-Access.
[3] Adam Satariano, *E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact*, N.Y. Times (July 16, 2020), https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html.

may have to comply with the European Union's General Data Protection Regulation (GDPR),[4] which includes a data deletion requirement.[5]

Further, even if the CDPA did raise compliance concerns for these businesses, there are more privacy-protective ways of addressing it than treating a deletion request as an opt out of sale. A narrower exemption based on CCPA regulations might read: "A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records."[6] This would help ensure that data brokers are able to delete a consumer's information if it is re-purchased.

Allowing data brokers to process deletion requests as an opt out of sale is inappropriate, because the retained data is vulnerable to data breaches. Indeed, RELX subsidiary LexisNexis, for example, has been breached, exposing consumers' personal information, multiple times.[7] Further, consumers typically are unable to control whether their information is collected by data brokers, as these companies buy and sell consumer data from other entities without having a direct relationship to the consumer. Consumers should have the choice to decide whether these companies keep their data within their systems.

Second, NICB asked for an exemption for non-profits for the purpose of fraud reporting to government entities. However, there is already a full exemption in the law for controllers and processors to "[p]revent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action[,]"[8] and to "[a]ssist another controller, processor, or third party with any of the obligations under this subsection."[9] Any additional exemption would be unnecessary, and harmful to consumers. At the very least, these organizations should be subject to transparency requirements so that consumers know the information that is being reported about them, and to have the opportunity to correct any errors.

Thank you for your consideration. We are happy to provide any additional information.

---

[4] *Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, European Data Protection Board (July 23, 2020) https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf.
[5] Art. 17 GDPR, https://gdpr-info.eu/art-17-gdpr/.
[6] Cal. Code Regs tit. 11 § 999.313(d)(3).
[7] Heather Timmons, *Security Breach at LexisNexis Now Appears Larger,* N.Y. Times (Apr. 13, 2005), https://www.nytimes.com/2005/04/13/technology/security-breach-at-lexisnexis-now-appears-larger.html; Byron Acohido, *LexisNexis Breach Reveals 'Secret Questions'*, USA Today (Sept. 27, 20130, https://www.usatoday.com/story/cybertruth/2013/09/27/lexisnexis-breach-reveals-secret-questions/2884625/.
[8] Va. Code Ann.§ 59.1-578(A)(7).
[9] *Id.* § 59.1-578(A)(9).

Sincerely,

Consumer Federation of America
Consumer Reports
Electronic Privacy Information Center
Privacy Rights Clearinghouse

cc: Members, Joint Commission on Technology and Science, Consumer Data Protection Work Group