

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:
ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON SECURITY

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

June 14, 2019

The Honorable Kevin McAleenan
Acting Secretary of Homeland Security
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528

Dear Acting Secretary McAleenan:

I write today regarding the reported data breach of a U.S. Customs and Border Protection (CBP) subcontractor, resulting in the exposure of photos of potentially tens of thousands of individuals' faces and license plates. Data breaches of any kind are alarming, but one of this magnitude that includes this type of personal data carries with it an even greater cause for concern.

The details of this data breach are highly troubling. According to a CBP statement, the compromised photos were taken at a land border crossing over the course of a month and a half, and the cyberattack targeted a CBP subcontractor's network, onto which the data had previously been downloaded.¹ CBP claims that fewer than 100,000 people were affected. However, the theft of a single individual's personal information is one theft too many, and given that data as sensitive as facial images was reportedly compromised, this breach is especially disturbing.

I have previously expressed concerns about the Department of Homeland Security's (DHS) biometric exit program and the privacy, security, and civil rights issues it raises. These sentiments are shared on a bipartisan basis. While DHS has not yet made clear whether the recent breach included data related to a facial recognition program, this episode is a clear example of the potential consequences of DHS' collection of sensitive personal data. These revelations further underscore the need to reassess what, if any, use of this technology should be allowed and to enact enforceable rules that 1) prioritize cybersecurity and personal privacy, 2) address potential discriminatory impacts of this technology, and 3) establish an effective process for U.S. citizens to opt out of this data collection altogether. DHS should pause its biometric data collection until such rules have been instituted.

¹ Drew Harwell & Geoffrey A. Fowler, *U.S. Customs and Border Protection says photos of travelers were taken in a data breach*, Wash. Post (June 10, 2019), https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/?utm_term=.29d4023b211d.

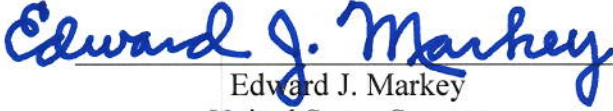
I have previously written to you with questions about the collection of biometric data. Those questions were driven by my concerns about both government overreach into individuals' zones of privacy and the possible targeting of that data by a variety of actors with bad intent. Both of those concerns are again implicated here. Accordingly, I request written answers to the following questions by July 8, 2019:

1. Please describe the process by which DHS collected the images that were exposed in this reported breach, the technology employed in this process, how long the images are stored, and the reason for this collection and storage.
2. How many images were breached? Please specify how many of these images were of individuals' faces, how many were of license plates, and how many were of other subjects.
3. Were the facial images exposed in this breach exclusively collected via biometric or license plate analysis tools, or did they also include images from personal documents such as personal ID cards?
4. Were the breached images in this episode linked to other pieces of personally identifiable information?
5. Has DHS confirmed the identity of the individual or entity that perpetrated this security breach? If so, please provide that information.
 - a. Does DHS have reason to believe that this attack was perpetrated by or in coordination with a foreign adversary?
 - b. Does DHS have reason to believe that this attack was perpetrated in order to extract a ransom from the subcontractor?
6. Has DHS coordinated with the Federal Bureau of Investigation or any other federal agency in response to this attack?
7. What written guidelines does DHS currently have regarding management of the type of data breached in this incident, including guidelines governing who can access the data, how long it is accessible, and for what purposes it can be used?
8. How many images of travelers' faces or license plates are DHS or any DHS contractors or subcontractors currently storing? For how long does DHS or its contractors store such information?
9. Does DHS policy require the agency and its partners to minimize the amount of data collected to the greatest extent possible? If such a policy does not exist, will DHS commit to implementing it?
10. What written guidelines does DHS currently have regarding its oversight of contractors (or subcontractors) and their data security practices?
11. What steps has DHS taken, including changes to its data management guidelines for contractors and subcontractors, to minimize the damage of this type of breach and to avoid future breaches of personal data?
12. Will DHS pause its deployment of any facial recognition and license plate analysis technology until it is able to ensure that any collected data is secure from abuse or hack? If not, why not?
13. Will DHS commit to notifying every individual whose information was compromised as a result of this data breach? If not, why not?

14. Will DHS commit to providing assistance, including but not limited to identity theft protection services, to all individuals affected by this data breach? If not, why not?
15. Will DHS commit to terminating its contracts with any company that violates the agency's security and privacy rules? If not, why not?

Thank you in advance for your attention to these requests. If you have any questions, please contact Bennett Butler of my staff at 202-224-2742.

Sincerely,



Edward J. Markey
United States Senator