

PATRICK J. LEAHY, VERMONT, CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
MAZIE HIRONO, HAWAII

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
JEFF FLAKE, ARIZONA

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Staff Director*
KRISTINE J. LUCIUS, *Chief Counsel and Deputy Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*
RITA LARI JOCHUM, *Republican Deputy Staff Director*

February 5, 2014

Kevin Alan Tussy
FacialNetwork.com
9065 South Pecos Road
Henderson, NV 89074

Dear Mr. Tussy:

I am writing to express my deep concern about your company's recently announced NameTag app for Google Glass. According to promotional materials, NameTag lets strangers get a broad range of personal information—including a person's name, photos, and dating website profiles—simply by looking at that person's face with the Glass camera. This is apparently done without that person's knowledge or consent, which crosses a bright line for privacy and personal safety. I urge you to delay this app's launch until best practices for facial recognition technology are established—a process that I've long called for and which begins tomorrow in Washington. At a minimum, NameTag should only identify people who have given the app permission to do so.

As Chairman of the Senate Judiciary Subcommittee on Privacy, Technology and the Law, I have serious concerns about facial recognition technology and how it might shape the future of privacy. Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere—on a lamppost across the street, attached to an unmanned aerial vehicle, or, now, integrated into the eyewear of a stranger.

No specific federal law governs this technology, so early adopter companies such as yours will play a vital role in determining the extent to which privacy and personal safety are protected. Your company has a duty to act as a responsible corporate citizen in deploying this technology, which must be done in a manner that respects and protects individual privacy. Tellingly, Google has chosen to prohibit facial recognition technology on Glass. How your company intends to address this prohibition remains unclear.

In 2012, I held a hearing in my subcommittee that looked at this sort of technology as it was on the verge of going mainstream. Carnegie Mellon Professor Alessandro Acquisti testified that he used off-the-shelf facial recognition software, combined with publicly available records, to successfully predict portions of people's Social Security numbers. Additionally, a Facebook representative refused to promise that his company would not share its facial recognition

database with third parties. This hearing established that the status quo is ripe for potential abuse by third parties who are willing to push the boundaries of privacy.

Since that hearing, concerns about facial recognition technology have only intensified. Notably, Facebook recently expanded its facial recognition database to include some of its least active users. By leveraging the photos of its one billion members, Facebook has likely amassed the world's largest privately-held database of faceprints. Yet the company still refuses to assure its users that it will not sell or share this database with third parties.

In response to these developments, I asked the National Telecommunications and Information Administration (NTIA) to study facial recognition technology. The NTIA will begin this study tomorrow at a meeting of industry and privacy experts in Washington, the first in a series of meetings called the Multistakeholder Process. The goal of this process is to produce consensus-driven best practices for facial recognition technology. I strongly urge you to postpone the launch of NameTag until the NTIA completes its study and best practices for this technology are established.

Additionally, I urge you to limit the app's facial recognition feature to only those individuals who have given their affirmative consent. Such an opt-in feature is a well-recognized best practice for mobile apps, but it is unclear whether NameTag will be opt-in.

I also have serious concerns that NameTag will be abused by bad actors. NameTag purports to make "the big, anonymous world we live in as friendly as a small town." But there can be safety in anonymity, and for many people, letting strangers identify them by name is a threat to that safety. I am especially concerned that NameTag plans to scan dating websites such as Match and OkCupid. It is easy to envision how this technology could facilitate harassment, stalking, and other threats to personal security. Your company has an obligation to protect users from these threats.

Finally, past experience indicates that NameTag could be a target for hackers. This vulnerability was underscored two years ago when Face.com, a company that was later acquired by Facebook, released the first commercial grade facial recognition program for public use. Although the program was designed to only identify the customer's Facebook friends, it was quickly hacked so that it could potentially be used to identify total strangers. If NameTag includes any privacy-protective features—which it should—your company needs to make assurances that they cannot be circumvented.

In light of these concerns, I respectfully request that you provide answers to the following questions:

1. Will NameTag be an opt-in program?
2. How are you addressing concerns that NameTag could be used by stalkers or other bad actors to jeopardize personal safety?

3. How does NameTag protect people who do not have an account from being identified? What are you doing to prevent hackers from circumventing these protections?
4. Which facial recognition database does NameTag use to identify faceprints? Is it owned by your company? If not, who owns the database?
5. Does NameTag use any Facebook photos, including public profile photos, to help identify individuals? What other websites are used?
6. Will you agree to adhere to the best practices established by the NTIA's Multistakeholder Process?
7. How do you plan to address Google's prohibition on facial recognition Glassware?
8. Do you intend to develop NameTag for other mobile devices, such as smartphones?

Thank you for your time and attention to these questions. I ask that you answer these questions within two weeks of receiving this letter.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

CC: The Honorable Lawrence E. Strickling
National Telecommunications and Information Administration