Statement of Commissioner J. Thomas Rosch, Dissenting in Part
What Facial Recognition Technology Means for Privacy and Civil Liberties
Testimony before the Senate Judiciary Subcommittee on Privacy, Technology and the Law
July 18, 2012

The Commission testimony expressly asserts that the staff will "release a report later this year setting forth best practices for using facial recognition technologies in a manner that respects consumer privacy."[1] The Commission testimony also expressly asserts that "[t]he Commission" intends to "release a report this year laying out recommended best practices" and dealing with whether "affirmative express consent" should be required "before engaging in facial recognition."[2] The testimony points out that in its March 2012 Privacy Report, the Commission previously identified such best practices and declared that "companies should provide consumers with choices" whenever data is collected that is "not consistent with the context of a transaction or a customer's relationship with a business," without narrowing the circumstances in which that may occur.[3] The Commission testimony very clearly telegraphs its intention to opine along these lines with respect to facial recognition.[4] Finally, the testimony is peppered with acknowledgments that privacy might be compromised by facial recognition technology but is not being compromised now.[5]

I look forward to seeing and reviewing the staff's final report on facial recognition technology. However, I will respectfully object if two recommendations find their way into a Commission report, at least until there is a lot more support for them.

First, I disagree with the notion that companies should be required to "provide consumers with choices" whenever "facial recognition" is used and is simply "not consistent with the context of a transaction or a consumer's relationship with a business."[6] As I noted when the Commission used the same language in its March 2012 Privacy Report, that would import an "opt-in" requirement in a broad swath of contexts. Furthermore, this result cannot be justified on

---

[1] Testimony at 3.

[2] *Id.* at 10-11.

[3] *Id.* at 9-10.

[4] *Id.* at 9-11.

[5] *See id.* at 5 ("possibly"); 7 (referring to "one company" that "only stores the aggregated demographic data" and "not images of the venues' customers"); 8 ("[a]s currently implemented, these features on social networks suggest 'tags' only of people that the user already knows"); 8 ("will it become feasible," and "[w]hile it does not seem that it is currently possible . . . it may be possible"), and 9 (asserting that "[s]ome have surmised," that "[i]f these predictions come to fruition," that facial recognition technology "could" compromise privacy).

[6] *Id.* at 10.

the ground that technological change will occur so rapidly with respect to facial recognition that the Commission cannot keep up with it when, as, and if a consumer's data security has been compromised or facial recognition has been used to build a consumer profile. There is no support at all in the Commission testimony for such a thesis, much less the kind of rigorous cost-benefit analysis that should be conducted before the Commission embraces an opt-in requirement. On the contrary, the Commission has shown that it can and will act promptly to protect consumers when that occurs.

Second, I similarly disagree with the adoption of "best practices" on the ground that facial recognition may be misused. There is nothing to establish that this misconduct has occurred or even that it is likely to occur in the near future. Beyond that, there is nothing in the Commission testimony resembling a cost-benefit analysis of adoption of these "best practices." Before that showing is made, it is at least premature for anyone, much less the Commission, to suggest to businesses that they should adopt as "best practices" safeguards that may be costly and inefficient against misconduct that may never occur.