Before the
National Telecommunications and Information Administration
Washington, DC

In the Matter of	)	
	)	
Developing the Administration's Approach to	)	WC Docket No. 180821780-8780-01
	)	
Consumer Privacy	)	

Comment by Elena Lucherini
Graduate Researcher
Princeton University

I am Elena Lucherini, a Computer Science graduate researcher at Princeton University. In this comment, I recommend that NTIA incorporate into its final policy that a business should not repurpose information provided by a consumer for security reasons unless the consumer gives explicit, opt-in consent. I support my comment by presenting my recent research about the privacy implications of Facebook's targeted advertising system, which allows advertisers to specify which users see their advertisements on the platform.

In my study of the Facebook Ads platform, I found that Facebook allows advertisers to target users with personally identifiable information that users provide for security purposes.[1] One of my main findings was that Facebook uses the phone numbers that consumers add to the platform specifically for two-factor authentication, or to receive alerts about new potentially hostile logins, as a means to target users with advertisements. When asked for comment, Facebook invited users who are bothered by this practice to use another means of two-factor authentication.[2]

The two-factor authentication alternative provided by Facebook, a mobile authentication application such as Google Authenticator, was only added in May 2018.[3] In order to set up two-factor authentication without a phone number, users are required to be sophisticated enough (and willing) to download and configure an application. While this alternative is considered more secure than two-factor authentication by SMS, it increases the complexity for non-expert users,

[1] G. Venkatadri, E. Lucherini, P. Sapiezynski, and A. Mislove. Investigating sources of PII used in Facebook's targeted advertising. https://mislove.org/publications/PII-PETS.pdf. In *Proceedings of the Privacy Enhancing Technologies Symposium (PETS'19)*, Stockholm, Sweden, Jul 2019.
[2] Facebook Is Giving Advertisers Access to Your Shadow Contact Information. https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051.
[3] Two-factor authentication for Facebook now easier to set up. https://www.facebook.com/notes/facebook-security/two-factor-authentication-for-facebook-now-easier-to-set-up/10155341377090766/.

who would potentially opt out of the feature altogether.[4] Furthermore, this may be perceived by consumers as a "lesson learned" that they cannot trust companies to not use their security-related personal data for other unexpected purposes. This may have negative effects on security across the board.

Privacy and security are two fundamental properties that should be able to coexist. I recommend that the NTIA expand its policy to include that a business should give clear notice of how it intends to use consumers' data. Even more critically, a business should obtain explicit opt-in consent from consumers if it wants to repurpose information provided in a security setting.

[4] B. Schneier. Two-factor authentication: too little, too late. In *Communications of the ACM - Transforming China*.