Facebook Statement to W5:

"We require people to use their real identities on Facebook and pretending to be someone else is an explicit violation of our policies. Imposter accounts affect real people, and we remove these accounts when we discover them. We've invested heavily in strengthening our technology to keep them off Facebook and we work with law enforcement to prosecute scammers. That job is not finished and we are committed to sharing our progress."

- Facebook company spokesperson

Additional background on romance scams and Facebook's efforts to combat them:

- Financially motivated scams, including romance scams, commonly rely on impersonating members of the public who are more likely to be considered trustworthy — including members of the military, veterans, and other professionals. As a result, these individuals are more likely to be targets of impersonation than most people on Facebook. We recognize this and factor it into our detection strategy.
- We remove large numbers of impersonating accounts on a consistent basis through a combination of technology, reporting tools and human review (more on this below). In particular, we are grateful to Kathy Waters and Bryan Denny for their diligence in regularly reporting these accounts to us. With their help, we are making progress in reducing the ability of scammers to impersonate people on our services.
- We work with law enforcement to help find and prosecute the scammers who conduct these activities. We also work to help raise awareness among the military community about impersonation.
- To help increase awareness of this issue, we published an educational video about detecting and reporting impersonation scams, including military impersonation, on the FB Military and Veterans Community Page (https://www.facebook.com/FBMilVetCommunity/): https://www.facebook.com/FBMilVetCommunity/videos/1655416797877942/. We also sent the video out to partners in the military community, both to generate awareness and so they could share the video more broadly using their own channels.
- We've seen that impersonation is not specific to any online platform, technology or group of people. As the Times has reported, it's a problem that pre-dates the internet and impersonation runs the gamut - scammers pretend to be celebrities, internet influencers, politicians and business executives.

Regarding Facebook's technology and policies used to remove imposter accounts:

- We are constantly iterating to improve our detection technology. We are **exploring new ways to strengthen our technology and processes** to combat impersonation; for example:
    - We're testing new detection capabilities to help quickly spot and remove accounts that pretend look like some of the most frequently impersonated members of the U.S. military and veterans. We do this by training our automated systems to look for certain techniques used by scammers to impersonate an individual, such as leaving out one letter of a person's name to make their imposter account look legitimate. We're still in the early stages of this testing but have seen promising results to date.
    - We are currently exploring ways to educate people within Messenger about how to stay safe from harmful behavior like scams and impersonation, and how to spot fake accounts. We hope to roll this out more broadly later this year.
- We have a dedicated team that works around the clock and across time zones to help detect and block fake accounts and content that violates our Community Standards.

    - In 2018 alone, we have **increased the number of people who work on security and safety issues** to more than 30,000.
- Our detection technology helps us **block millions of attempts to create fake accounts every day** and detect millions more often within minutes after creation. Our systems examine thousands of account attributes and focus on detecting behaviors that are very difficult for bad actors to fake, including their connections to others on our platform.
    - In our latest Community Standards Enforcement Report, we reported that **we removed 2.19 billion fake accounts in Q1, up from 1.2 billion in Q4 last year.** This is due to an increase in automated attacks by bad actors who try to create large amounts of fake accounts at a time but most of these accounts were blocked within minutes of their creation before they can do any harm, and were removed so soon they were never considered active.
- We've made several improvements to our technology help combat impersonation:
    - **Machine learning:** In March 2018 we introduced new machine learning techniques that **helped us take action on more than a half-million accounts tied to financial scams on Facebook**. These machine learning techniques get more effective over time as they process additional cases. When our systems assess that an account is likely associated with scam behavior, the account owner must complete a few actions to demonstrate that they are not operating a fake account or misrepresenting themselves. Until they do this, the account can't be used to reach others. If the owner fails the verification, or if our Community Operations team determines that there is a violation of our policies, the account will be removed. See: https://www.facebook.com/notes/facebook-security/introducing-new-machine-learning-techniques-to-help-stop-scams/10155213964780766/
    - **Impostor reporting:** You can report an impostor account on Facebook whether or not you have an account. We created a dedicated help center link to report imposters on Facebook, Instagram, and Messenger at: facebook.com/help/fakeaccount