THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY of WASHINGTON

TASK FORCE 2017

Extremist Use of Social Media: Balancing Privacy & National Cybersecurity

BECAUSE THE REALM OF CYBERSECURITY IS CONSTANTLY CHANGING, THERE IS A DISCONNECTION TODAY BETWEEN GOVERNMENT AND INDUSTRY ON THE ISSUES OF PRIVACY AND NATIONAL SECURITY. INDUSTRY AND GOVERNMENT MUST BALANCE SOCIAL MEDIA USAGE BY ACTIVISTS AND ORDINARY PEOPLE WITH EXTREMIST AND TERRORIST USAGE FOR RECRUITMENT AND COMMUNICATION EFFORTS.

ISSUE DESCRIPTION

THE DISCONNECTION BETWEEN GOVERNMENT AND INDUSTRIES HAS MADE IT EASY FOR EXTREMISTS TO USE SOCIAL MEDIA PLATFORMS TO RECRUIT AND COMMUNICATE.

- International terrorist groups, such as ISIS, use the Internet to great effect, recruiting potential members and communicating about attacks. Extremist Internet use includes savvy social media and mobile technology use. In response, the U.S. government has asked technology companies to help it manage this problem through use of content moderation, content monitoring, and providing law enforcement with backdoors into products.

- Technology companies have attempted to assist the government in many of its requests, but also often "push back" over concerns that the government's desire to monitor potential terrorists will lead to ordinary consumers' rights to privacy and expression being violated. Law in the U.S. around this issue remains undeveloped.

- There is a need of solution to allow law enforcement to protect citizens while also protecting the rights of activists and ordinary people.

POLICY RECOMMENDATIONS

- The government should sponsor an ad-campaign that outlines how to know when someone is in communication with extremists via social media and advises individuals on how to approach the situation and report such instances. Moreover, early education of children and young adults should focus on Internet safety and how to recognize the signs of extremism online and in their peers.

- Law enforcement and intelligence agencies should be given the authority to legally collect the information necessary for national security on any US or non-US person, if and only if, the person or persons in question present a clear and present danger or have close ties to someone who presents a clear and present danger.

- Law enforcement and intelligence agencies should be given the authority to legally collect the information necessary for national security on any US or non-US person, if and only if, the person or persons in question present a clear and present danger or have close ties to someone who presents a clear and present danger.

TASK FORCE ADVISOR

Jessica Beyer

TASK FORCE MEMBERS

Jane Birkeland
Jordan Johnson
Serena Eunbich Ko
Kristy Soo Jung Kwon
Taelim Leena Lee
Natalie Meek
Tae-Hyun Thomas Park
Phoibe Purcell
Cameron Rosenberg
Hannah Ross
Rajeev Stephens
Marielle Trumbauer
Priya Uppal
Xingyue Yang
Julia Yoon

TASK FORCE EVALUATOR

Paul Nicholas

Senior Director,
Microsoft Trustworthy Computing