MEMO TO: Senators of the Senate Select Committee on Intelligence
MEMO FROM: Phil Howard, Oxford Internet Institute
MEMO REGARDING: Questions for the Record
MEMO DATE: 04/09/2018

Thank you for the opportunity to respond to more questions. I prefer to stick to the evidence that we in the Project on Computational Propaganda at the Oxford Internet Institute have been collecting and analyzing. So my answers on the long history of Russian propaganda mostly focus on the contemporary trends and evidence that I am familiar with.

Questions from Senator Cotton

1) Aren't the themes the KGB used in 1982, similar to those we're seeing the Russian Intelligence Services use on social media in 2018?

Some of the themes in today's Russian misinformation campaigns are consistent with previous campaigns, but there are four important differences. First, there are some unusual new themes, many of which are about discouraging voters from trusting evidence, science, or the expertise of their political leaders. For example, there are campaigns to discourage parents in the US from inoculating their kids against diseases. There are campaigns to get people to distrust the science and evidence on things like climate change and healthy nutrition. Second, the propaganda is delivered in a different way. KGB propaganda messages from 30 years ago reached far fewer people, often indirectly, not in a targeted way, and rarely through US media itself. Today, US-based social media companies deliver the content, reaching more people in direct and targeted ways. Third, I think the propaganda attacking two key democratic institutions—journalism and elections—is new. The campaigns to undermine trust in news organizations, independent journalism, elections administrators and public officials are a contemporary phenomenon. Most of the previous Russian propaganda was focused on particular issues and the interpretation of events. This new propaganda is focused on particular democratic processes and institutions. Fourth, the form of political speech is different. US voters had a right to hear the opinions of other governments about world affairs thirty years ago. Contemporary disinformation is so full of lies and disinformation it probably does not warrant the same free speech protections.

2) Isn't this Russian social media campaign really just old wine in new bottles, with perhaps a different distributor?

This metaphor is close but not quite right. The bottles are labelled as wine, but the bottles contain poison and the poison is being distributed over networks of family and friends.

3) To what extent have you looked for and seen Russian activity on this front on social media?

Efforts to undermine trust in the military, nuclear modernization efforts, and sow distrust between the US and NATO continue. But yet another difference is that campaigns of misinformation on national security issues can now be directly targeted at active duty military personnel, veterans, and their friends and family. In our research memo "Junk News on Military Affairs and National Security" we make three observations. First, over Twitter we find that there are significant and persistent interactions between

current and former military personnel and a broad network of extremist, Russia-focused, and international conspiracy subgroups. Second, over Facebook, we find significant and persistent interactions between public pages for military and veterans and subgroups dedicated to political conspiracy, and both sides of the political spectrum. Third, over Facebook, the users who are most interested in conspiracy theories and the political right seem to be distributing the most junk news, whereas users who are either in the military or are veterans are among the most sophisticated news consumers, and share very little junk news through the network.

Questions from Senator Manchin

4) What modifications would you recommend to the large social media companies that would enable users to identify the source and potential funding of items posted on social media?

I believe users should have access to two kinds of information: (I) the sources of funding that pay for the ads they see; (II) the ultimate beneficiaries of user data. This means that users should be able to go into their account profile and see a list of the organizations that have paid to place ads directed to them. It means that users should be able to see a list of the third party data mining firms, advertising firms, political actors, and foreign governments that are making use of data the user generated by using the social media platform.

5) Should there be disclaimers on anything other than personal information?

It would be great if users could explore the sources of all ads and content they are served. But this would be a huge volume of information so I believe it best to start with political news, information and ads.

6) Should everything posted on social media have a "tag" that allows users to determine who posted information, even if it was re-posted or shared by another person, so you can always determine the actual source?

Tracking the ultimate source of an ad or post would be interesting to some users. But most people post of the time don't think about politics. They turn to politics when there is an election or crisis brewing, and professional news outlets are working hard to draw public attention to current events.
At election time, or during those sensitive political moments, users are more likely to want to know which lobbyists, political parties, candidates or PACs are benefiting from the data they have generated as users.

Questions from Senator King

7) At the hearing on August 1, 2018, I asked each witness to submit written policy recommendations to the Committee. Specifically, please provide recommendations on the following topics:
    a. Technical solutions, such as requirements to label bot activity or
    b. identify inauthentic accounts;
    c. Public initiatives focused on building media literacy;
    d. Solutions to increase deterrence against foreign manipulation;
    e. Any additional policy recommendations.

There are two ways to protect democracy from the challenge posed by tech companies' dominance over socially valuable data. The first option is for governments to regulate content on an unprecedented scale. That would oblige public regulators to either review all social media content to judge its appropriateness or provide clear signals to private firms — whether the social media companies themselves or third parties — to perform such content reviews. But the problem with both scenarios is that they would create massive new censorship mechanisms that would further threaten democratic culture.

Far preferable would be market regulations that guide firms on how and when they can profit from information about individuals. Such regulations would put the public back in charge of a valuable collective resource while still allowing citizens to express themselves individually by deciding what to do with their data. To get there, policymakers should focus on five basic reforms, all of which would put public institutions back into the flow of data now dominated by private firms.

First, governments should require mandatory reporting about the ultimate beneficiaries of data. That means, when queried, technology firms should be required to clearly report to users which advertisers, data miners, and political consultants have made use of information about them. Your Facebook app or your smart refrigerator should be required to reveal, on request, the list of third parties benefiting from the information the device is collecting. The trail of data should be fully, and clearly, mapped out for users so that if a data-mining firm aggregates users' data and then sells it on to a political party, the users could still identify the ultimate beneficiary.

Second, regulations should require social media platforms to facilitate data donation, empowering users to actively identify the civic groups, political parties, or medical researchers they want to support by sharing data with them. In freeing data from private actors, governments could create an opportunity for civic expression by allowing citizens to share it with whichever organizations and causes they want to support — not just the ones that can afford to buy it, as is the case today. Making data fully portable is only partly about creating some market opportunities for new startups, it is about allowing users to volunteer, participate and engage in a modern way, by contributing to the their data to the civic and public groups they want to support.

The third reform is related to the second: Software and information infrastructure companies should be obliged to tithe for the public good. Ten percent of ads on social media platforms should be reserved for public service announcements, and 10 percent of all user data should be obliged to flow (in a secured way) to public health researchers, civic groups, professional journalists, educators, and public science agencies. Such a system would allow many kinds of advocacy groups and public agencies, beyond the social media firm's private clients, to use existing data to understand and find solutions for public problems.

Fourth, the nonprofit rule on data needs to be expanded. Most democracies have rules that prevent firms from profiting from the sale of certain kinds of public data. In many US states, for example, data-mining firms can't profit from the sale of voter registration data, which public agencies collect. This rule needs to be extended to a wider range of socially valuable data, like much of that collected in the US census, but is now gathered and held by technology companies. Such classes of information could then be passed to public agencies, thus creating a broader set of data in the public domain.

Fifth, public agencies should conduct regular audits of social media algorithms and other automated systems that citizens now rely on for information. Technology companies will call these algorithms

proprietary, but public agencies currently audit everything from video gambling machines to financial trading algorithms, all in ways that don't violate intellectual property. Many kinds of political actors have accused technology firms of ideologically biased search and news algorithms. Usually such accusations are baseless, and the deeper problem is misinformation and computational propaganda. Independent review would help us all trust social media and ultimately our political institutions.

Users should have access to clear explanations of the algorithms that determine what news and advertisements they are exposed to, and those explanations should be confirmed by regular public audits. Moreover, all ads, not just political ones, need to be archived for potential use by public investigators. Audits of today's technology would also put the designers of new technologies — such as artificial intelligence — on notice that their own algorithms will one day be under scrutiny.