The Washington Post

Opinions

Russians are hacking our public-commenting system, too

By Jessica Rosenworcel March 6

Jessica Rosenworcel is a member of the Federal Communications Commission.

What do Sen. Jeff Merkley (D-Ore.), deceased actress Patty Duke, a 13-year-old from upstate New York and a 96-year-old veteran from Southern California have in common?

They appear to have filed comments in the net neutrality record at the Federal Communications Commission. That ought to mean they went online, submitted their names and addresses, and typed out their thoughts about Internet regulatory policy. But appearances can be deceiving. In fact, each of these individuals — along with 2 million others — had their identities stolen and used to file fake comments.

These fake comments were not the only unnerving thing in the FCC net neutrality record. In the course of its deliberations on the future of Internet openness, the agency logged about half a million comments sent from Russian email addresses. It received nearly 8 million comments from email domains associated with FakeMailGenerator.com with almost identical wording.

Unfortunately, this was not an isolated case. Researchers, journalists, and public servants have found a wide range of fake comments and stolen identities in the public proceedings of the Labor Department, Consumer Financial Protection Bureau, Federal Energy Regulatory Commission, and Securities and Exchange Commission.

This is a serious problem. Administrative decisions made in Washington affect Americans' day-to-day lives and future. They involve everything from Internet access to retirement planning to the availability of loans to the energy sources that power our homes and businesses.

Since 1946, the Administrative Procedure Act has required agencies making decisions on major policy changes to open their process to the public. They are required to give "interested persons" an opportunity to voice their opinions, and only after considering these public comments may agencies proceed with proposed policies and adopt new rules.

This system served us well for decades, but it is growing creaky and showing its age. In proceedings at the FCC and elsewhere, it is apparent that the public is increasingly shut out of decision-making by the fraud that is flooding public channels for comment. And it's a good bet that this is only going to get worse. The mechanization and weaponization of the comment-filing process have only just begun.

No one said digital age democracy was going to be easy. But it's time to brace ourselves and strengthen our civic infrastructure to withstand what is underway. This is true across government. You can find disturbing parallels between the flood of fake comments in regulatory proceedings and the barrage of posts on social media that was part of a now-infamous campaign to influence the 2016 presidential election. In short, there is a concerted effort to exploit our openness. It deserves a concerted response.

This has not yet happened. At the FCC, for instance, anyone who has found their name stolen and misused in the net neutrality docket has been advised to file another statement to that effect in the public record. This is too narrow a solution for such a monumental problem.

Moreover, in its latest budget request, the agency has not pursued any funding to improve the security of our public comment system. This is hard to fathom. At a minimum, the FCC, like other agencies, should be requesting funds to study the scope of fraud in its public process and putting in place simple security measures like CAPTCHA or two-factor authentication.

Even more alarming, the agency has refused to work with those who want to get to the bottom of this mess, such as the attorney general of New York, who has found that tens of thousands of residents in his state — as well as in California, Georgia, Missouri, Ohio, Pennsylvania and Texas — have had their identities stolen. This is not right. Identity theft is a violation of both state and federal law.

In January, the Government Accountability Office announced that it would be reviewing the "extent and pervasiveness of fraud and the misuse of American identities during the federal rulemaking process." The letter noted the investigation could not begin for five months. That's a start. But it's not enough.

We need a lot more investigating, including from the Justice Department and the FBI. The sheer volume of fraud suggests a systemic effort to corrupt the process by which the public participates in some of the biggest decisions made in Washington. That deserves attention — and a fix. If we do this right, we can do more than rid our public records of comments from dead people and Russia, stolen identities and bots. We can find a way to give all Americans — no matter who they are or where they live — a fighting chance at making Washington listen to what they think.

Read more:

The Post's View:The growing scourge of cybercrime demands action from Congress

Paul Waldman: Russia is going to attack our next election. The Trump administration may not even try to stop it.

Letters to the Editor: With CAPTCHA toppled, it's time to rethink artificial intelligence

Jessica Rich: The false promise behind the FCC’s net neutrality repeal plan

Robert D. Kaplan: Everything here is fake

261 Comments