From:	Tim Ridout
To:	iotrfc2017
Subject:	IOT RFC 2017
Date:	Saturday, February 25, 2017 5:17:50 PM

Dear Sir or Madam,

I appreciate the work you are doing on IoT and the opportunity to comment on the report, FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS. The discussion itself strikes me as fairly comprehensive. With IoT, as with all Internet-connected electronics, the difficulty is how to minimize negative externalities -- i.e., those costs borne collectively that are not captured by the market but which are quite real -- in a large and growing ecosystem where responsibility is often diffused among myriad actors, many of whom shirk accountability. Finding a way to capture those costs and assign liability in order to encourage responsible best practices could be a more effective means rather than detailed command-and-control regulations that will never be able to keep up with rapidly evolving technology.

With this in mind, I suggest encouraging the growth of independent ratings agencies akin to those in the financial sector, which could focus their attention on software developers, device manufacturers, and system architects, developing an easily understood and trusted rating system that would closely follow emerging best practices for security and periodically re-assess how well companies are doing. These ratings could be linked to the emerging cyber insurance market, which would factor the cost of negative externalities into their insurance premiums. Of course, liability would need to be assigned to manufacturers, system architects, network administrators, and perhaps even users in such a way that encouraged best behavior in a fair and cost-effective way that took into account the most common points of failure/security breaches. Additionally, basic consumer labeling and usage instructions that are intelligible to non-technical users should be required, as should strong, randomized default passwords.

As with most policy questions, where to place the burden of responsibility is contentious. But it is fantasy to presume that the average consumer will ever be able to keep up with the latest technical specifics and be able to do much more than follow best practices on passwords and automatic software updates. Besides, there is a division of labor in society and specialization exists for a reason. Expecting all users to become computer security experts will never work, especially since the systems themselves keep changing. Encouraging best practices through education and labeling, and providing a centralized "clearing house" of key information for consumers could be very useful, but liability will ultimately have to lie with system architects, network administrators, and device manufacturers -- even if they ultimately have to pass some of those costs onto consumers. NIST and other agencies should continue to promulgate guidelines, but encouraging independent ratings agencies and cyber insurance markets could help fill in the security gaps that make us all vulnerable. With a system in place to more effectively manage the negatives which is designed to be adaptive, IoT companies could be free to grow and innovate in a less anarchic, but not overly burdensome environment.

Thank you for the work you do.

Sincerely,
Tim Ridout