Dear Target, Walmart, Best Buy and Amazon -

The advent of new connected consumer products offers many benefits. However, as you are aware, there are also serious concerns regarding standards of privacy and security with these products. These require urgent attention if we are to maintain consumer trust in this market.

It is estimated that by 2020, 10 billion IoT products will be active.[1] The majority of these will be in the hands of consumers.[2] Given the enormous growth of this space, and because so many of these products are entrusted with private information and conversations, it is incredibly important that we all work together to ensure that internet-enabled devices enhance consumers' trust.

Cloudpets illustrated the problem, however we continue to see connected devices that fail to meet the basic privacy and security thresholds. We are especially concerned about how these issues impact children, in the case of connected toys and other devices that children interact with. That's why we're asking you to publicly endorse these minimum security and privacy guidelines, and commit publicly to use them to vet any products your company sells to consumers. While many products can and should be expected to meet a high set of privacy and security standards, these minimum requirements are a strong start that every reputable consumer company must be expected to meet. These minimum guidelines[3] require all IoT devices to have:

1) Encrypted communications
The product must use encryption for all of its network communications functions and capabilities. This ensures that all communications are not eavesdropped or modified in transit.

2) Security updates
The product must support automatic updates for a reasonable period after sale, and be enabled by default. This ensures that when a vulnerability is known, the vendor can make security updates available for consumers, which are verified (using some form of cryptography) and then installed seamlessly. Updates must not make the product unavailable for an extended period.

3) Strong passwords
If the product uses passwords for remote authentication, it must require that strong passwords are used, including having password strength requirements. Any non-unique default passwords must also be reset as part of the device's initial setup. This helps protect

[1] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[2] *Gartner Says 8.4 Billions Connected "Things" Will be in Use in 2017, Up 31 Percent from 2017*, Gartner (Feb. 17, 2017), http://www.gartner.com/newsroom/id/3598917.

[3] For full guidelines please see:
https://medium.com/read-write-participate/minimum-standards-for-tackling-iot-security-70f90b37f2d5

the device from vulnerability to guessable password attacks, which could result in device compromise.

4) Vulnerability management
The vendor must have a system in place to manage vulnerabilities in the product. This must also include a point of contact for reporting vulnerabilities and a vulnerability handling process internally to fix them once reported. This ensures that vendors are actively managing vulnerabilities throughout the product's lifecycle.

5) Privacy practices
The product must have a privacy policy that is easily accessible, written in language that is easily understood and appropriate for the person using the device or service at the point of sale. At a minimum, users should be notified about substantive changes to the policy. If data is being collected, transmitted or shared for marketing purposes, that should be clear to users and, in line with the EU's General Data Protection Regulation (GDPR), there should be a way to opt-out of such practices. Users should also have a way to delete their data and account. Additionally, like in GDPR, this should include a policy setting standard retention periods wherever possible.

We've seen headline after headline about privacy and security failings in the IoT space. And it is often the same mistakes that have led to people's private moments, conversations, and information being compromised. Given the value and trust that consumers place in your company, you have a uniquely important role in addressing this problem and helping to build a more secure, connected future. Consumers can and should be confident that, when they buy a device from you, that device will not compromise their privacy and security. Signing on to these minimum guidelines is the first step to turn the tide and build trust in this space.

Yours,

Mozilla
Internet Society
Consumers International
ColorOfChange
Open Media & Information Companies Initiative
Common Sense Media
Story of Stuff
Center for Democracy and Technology
Consumer Federation of America
18 Million Rising
Hollaback