WHAT IS THE DIGITAL STANDARD?

New America's Open Technology Institute (OTI) has begun a new project centered on promoting and educating both corporations and civil society about the new privacy and security testing regimen called The Digital Standard.[1]

We are focused on ensuring the Standard's maximum impact by working across many constituencies to use and refine this tool as a metric for evaluating consumer software and hardware. Our goals are to educate companies on how they can use the Standard to improve their products, help consumer and digital rights advocates to leverage the Standard in their advocacy, and solicit feedback from the full range of stakeholders on how the Standard can be improved.

When consumers buy a new device for their homes that connects to the internet, like a smart TV or refrigerator, they may not be thinking about the privacy and security risks that come with it. But providing customers tools to help evaluate the security and privacy of the devices that they choose to let into their digital and–even more these days–their physical lives, can make a big impact on the products they choose to purchase. From the video baby monitor we buy, to the thermostat we install and the television that we watch, we should not have to be concerned that these devices are able to share our private lives with anyone on the internet with access to the default password. Companies are being given access to reams of private information about their customers, and they have a responsibility to ensure its security, or risk losing their customers and their reputation.

The Digital Standard is an example of an ambitious, open, and collaborative effort to create a digital privacy and security standard to help guide the future design of consumer software, digital platforms and services, and internet-connected products.

What is the Digital Standard?

The Digital Standard, a collective effort led by **Consumer Reports**, **Disconnect**, **Ranking Digital Rights**, and **The Cyber Independent Testing Lab**, with assistance from Aspiration, is a set of individual tests that taken together form a methodology for evaluating the privacy and security impacts of a given piece of software or hardware. It was created to define and reflect important consumer values that must be addressed in the development of software and hardware products. The Standard is underpinned by a set of guiding principles: electronics and software-based products should be secure, consumer information should be kept private, ownership rights of consumers should be maintained, and products should be designed to combat harassment and help protect freedom of expression.

The Standard's methodology is composed of 35 different "tests" that can be used to measure products to see how their design and policies meet best practices for digital privacy and security. It also provides a model that companies can use to design and improve their products, ensuring that they are best in class on these issues and giving them an opportunity for product promotion in a crowded field.

The Digital Standard is an open source, collective effort which seeks participation from a broad community of researchers, testers, and manufacturers.

To provide feedback on our project, please visit: **tiny.cc/raisingthestandard**

What does the Digital Standard do?

The Digital Standard addresses eight themes, which can be used when developing and evaluating products. Although the methodology itself is highly granular, allowing nuanced tests to be performed against specific criteria, for education and design purposes it is useful to divide the methodology by topic. Companies will be evaluated by a set of indicators in each thematic area and must fulfill certain requirements to be certified as employing best digital security and privacy practices.

Encryption

Information that users provide to the device or company should be encrypted. Customer information that is transmitted should be encrypted and use unique encryption keys, and the product should have the ability to implement end-to-end encryption.

Vulnerabilities

Companies should have a mechanism that allows independent researchers to report vulnerabilities in their products, and publicly discloses the timeframe in which it will review these reports. They also should commit to not taking legal action against researchers who report using this process. In order to help protect against persistent software vulnerabilities, companies should test against all known vulnerabilities and consider using open source code for critical security libraries.

Passwords

Product passwords should be unique and the customer should have the ability to change them. They should be required to be of a certain length and complexity, and only able to be modified using the existing product password.

User Data

The company is transparent about exactly what data it is collecting, and does not collect more information than is necessary to use the service. Users are made aware of what data are being shared, and with whom - including government or legal authorities. The company is also clear about how long it retains that data, and ensure that all user information is deleted after users terminate their account or remove service from a device.

Threat Notification

The company clearly discloses its process for notifying customers who might be affected by a data breach, and commits to notifying the relevant authorities without undue delay when a data breach occurs. The company also clearly discloses what kinds of steps it will take to address the impact of a data breach on its users.

Terms of Service

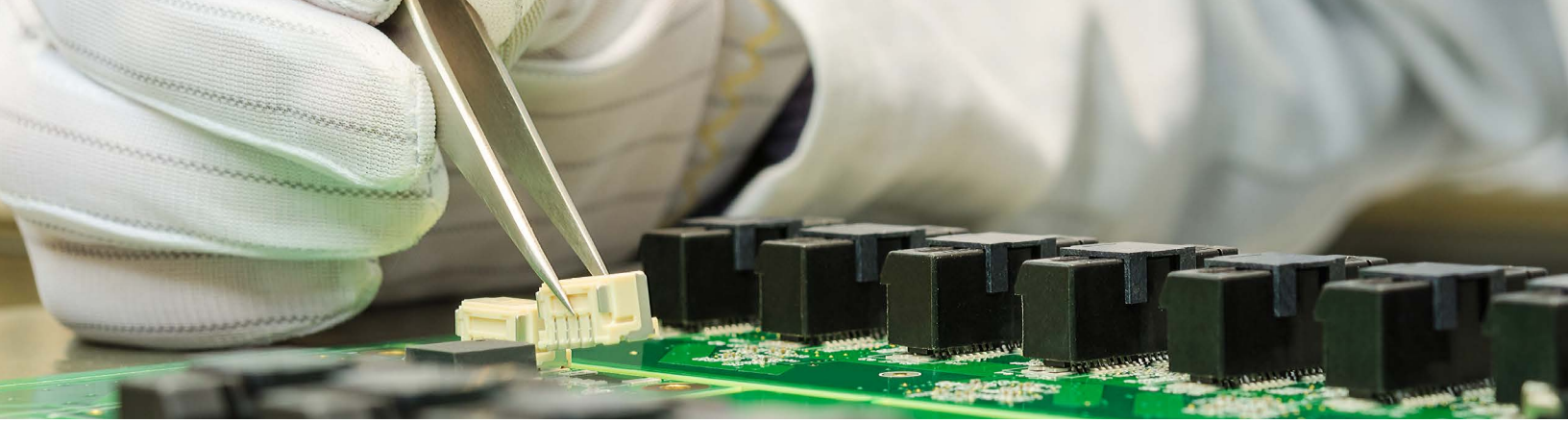
Users can easily find, read, and understand the terms of service and will receive notification if those terms are changed. It is also clear when, why, and how often the company enforces those terms of service and unilaterally closes user accounts.

Transparency

The company releases reporting data at least once a year disclosing information like the number of government requests for information it receives by country, the number of accounts affected, the number of requests it complied with, and what types of government requests it is prohibited by law from disclosing. It is also transparent about its practices for sharing user data with the government and other third parties.

Governance

The company has an explicit and clearly articulated policy commitment to human rights, including freedom of expression and privacy. It should also ensure that it has a transparent process for collecting and responding to complaints related to freedom of expression and privacy, and clearly communicate information about how it is responding to these complaints.



Why should companies care about privacy and security?

In 2018, companies who produce network-connected products, or any products that collect customers' private information, need to treat their users' privacy and security as a serious priority. Creating more secure technology is important from a cybersecurity perspective, to protect devices and networks from data breaches, attacks by hackers, or massive technical failures, but is also just good business strategy for companies. The economic and public relations impacts of insecure products on business operations, continuity, and solvency can be enormous, and they are only likely to increase as regulators around the world grow bolder in addressing security lapses as serious consumer protection problems. For example:

- The Ponemon Institute, a U.S. research firm, estimated that the average data breach in 2017 cost the responsible business $3.5 million;[2]
- In October of 2016, a botnet made up of compromised Internet of Things devices disabled large portions of the internet by taking out popular Domain Name Service provider Dyn, costing untold millions across the internet services space and prompting questions about liability;[3]
- The Federal Trade Commission, the United State's primary consumer protection agency, has a long list of enforcement actions based on inadequate security in products ranging from home broadband routers to electronic health record systems, and which regularly carry 20-year auditing obligations and monetary fines. Security breaches could cost manufacturers millions of dollars in FTC penalties;[4]
- Consumer Reports, one of the most trusted reviewers of consumer products, has announced their intention to begin considering the security and privacy of the products they evaluate;[5]
- The Digital Standard could become a marketing tool to evaluate the security of internet-connected devices. Companies in other industries use popular certification systems like Energy Star or LEED to attract customers. For example, condominiums in LEED-certified buildings sell for 21% more than analogous properties without the certification.[6]

[1] "The Digital Standard," available at **https://www.thedigitalstandard.org/**.

[2] "2017 Ponemon Cost of Data Breach Study" Ponemon Institute, available at **https://www.ibm.com/security/data-breach**.

[3] "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," *Krebs on Security*, October 21, 2016, **https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/**.

[4] In the Matter of Uber Technologies, Inc, FTC MATTER/FILE NUMBER: 152 3054, August 21, 2017, available at **https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc**.

[5] "Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds," Consumer Reports, February 7, 2018, **https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds**.

[6] Kerry Curry, "People Are Paying a 20% Premium for 'Green' LEED-Certified Condos," accessed July 28, 2017, **http://www.mansionglobal.com/articles/26952-people-are-paying-a-20-premium-for-green-leed-certified-condos**.

Who are we?

New America's Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators. Find out more at **www.newamerica.org/oti**.

NEW AMERICA

OPEN TECHNOLOGY INSTITUTE

To provide feedback on our project, please visit: **tiny.cc/raisingthestandard**