INTERNET OF THINGS PRIVACY, SECURITY AND GOVERNANCE

New devices, new vulnerabilities

The attributes of many IoT devices present new and unique security challenges compared to traditional computing systems.

- **Device Cost/Size/Functionality**
- **Volume of identical devices (homogeneity)**
- **Long service life (often extending far beyond supported lifetime)**
- **No or limited upgradability or patching**
- **Physical security vulnerabilities**
- **Access**
- **Limited user interfaces (UI)**
- **Limited visibility into, or control over, internal workings**
- **Embedded devices**
- **Unintended uses**

Key Challenge: IoT Ecosystem

Three Dimensions:

- Combination of devices, apps, platforms & services
- Data flows, touch points & disclosures
- Lack of defined standards

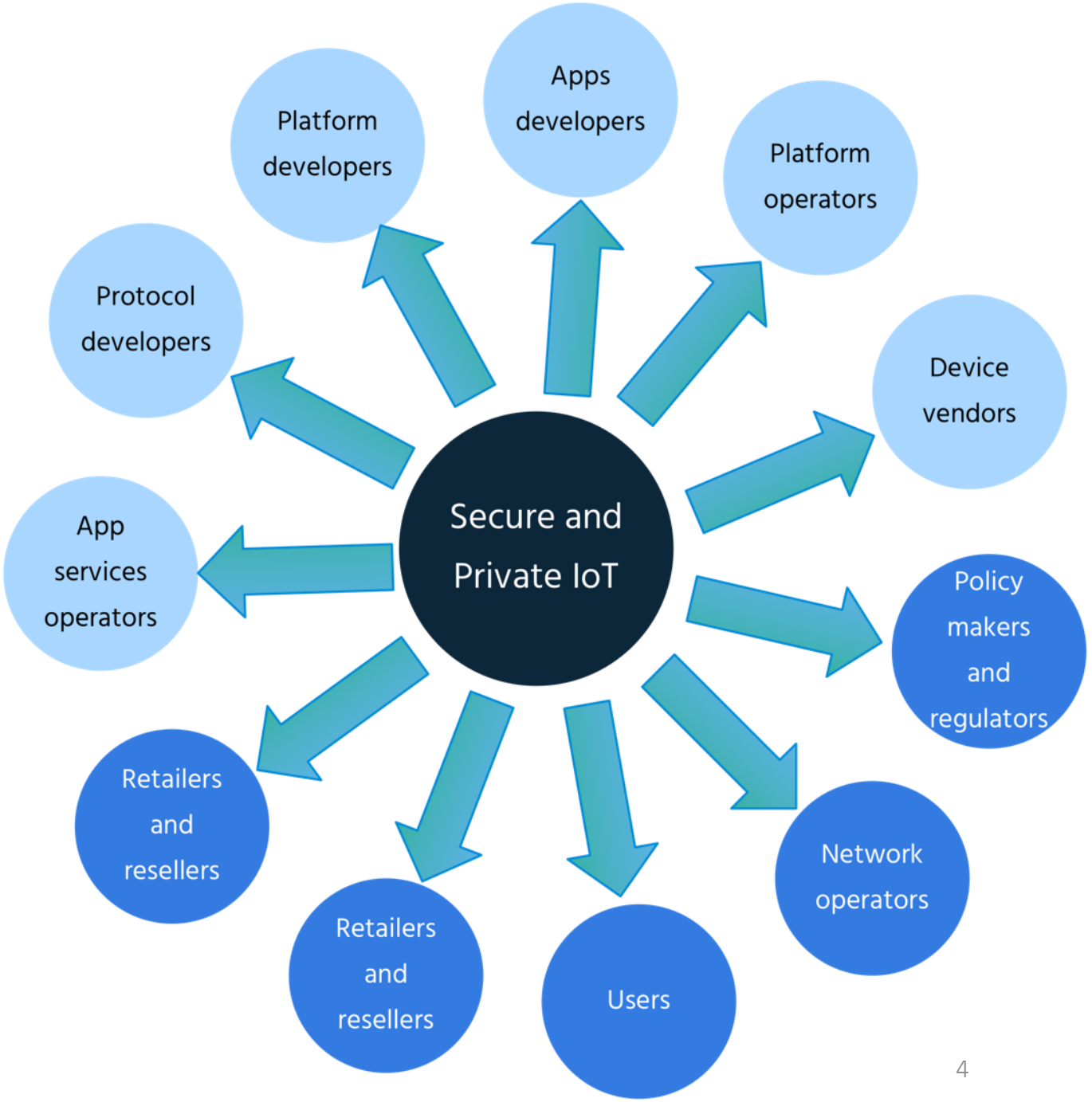
Impacts on Sustainability Issues:

- Lifecycle supportability
- Data retention / ownership

Who is responsible?

- **Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm**

- To scale up we need a collective approach, addressing security challenges on all fronts.

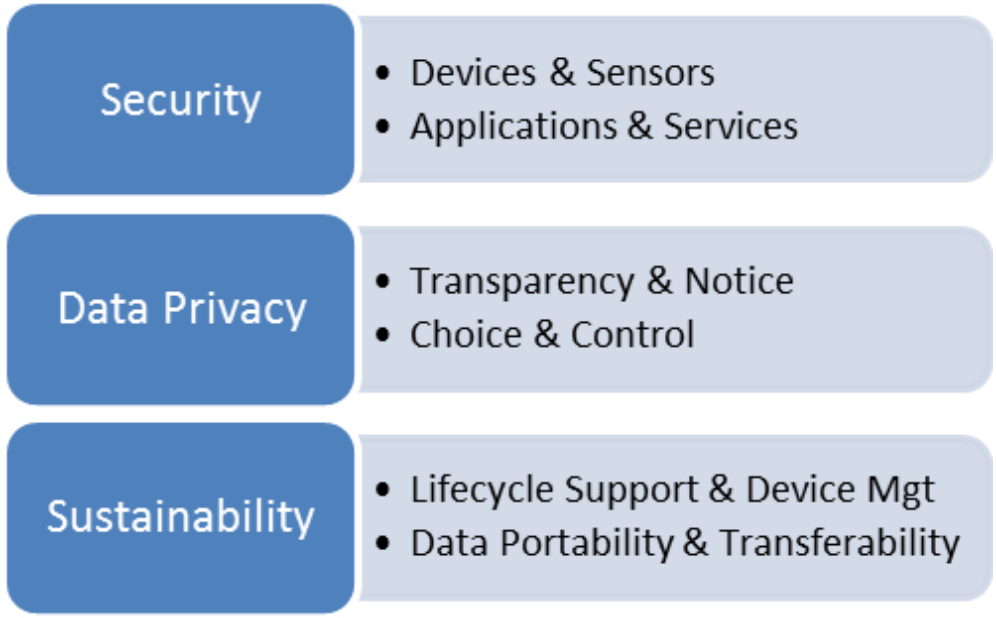


There are two ways to view IoT Security

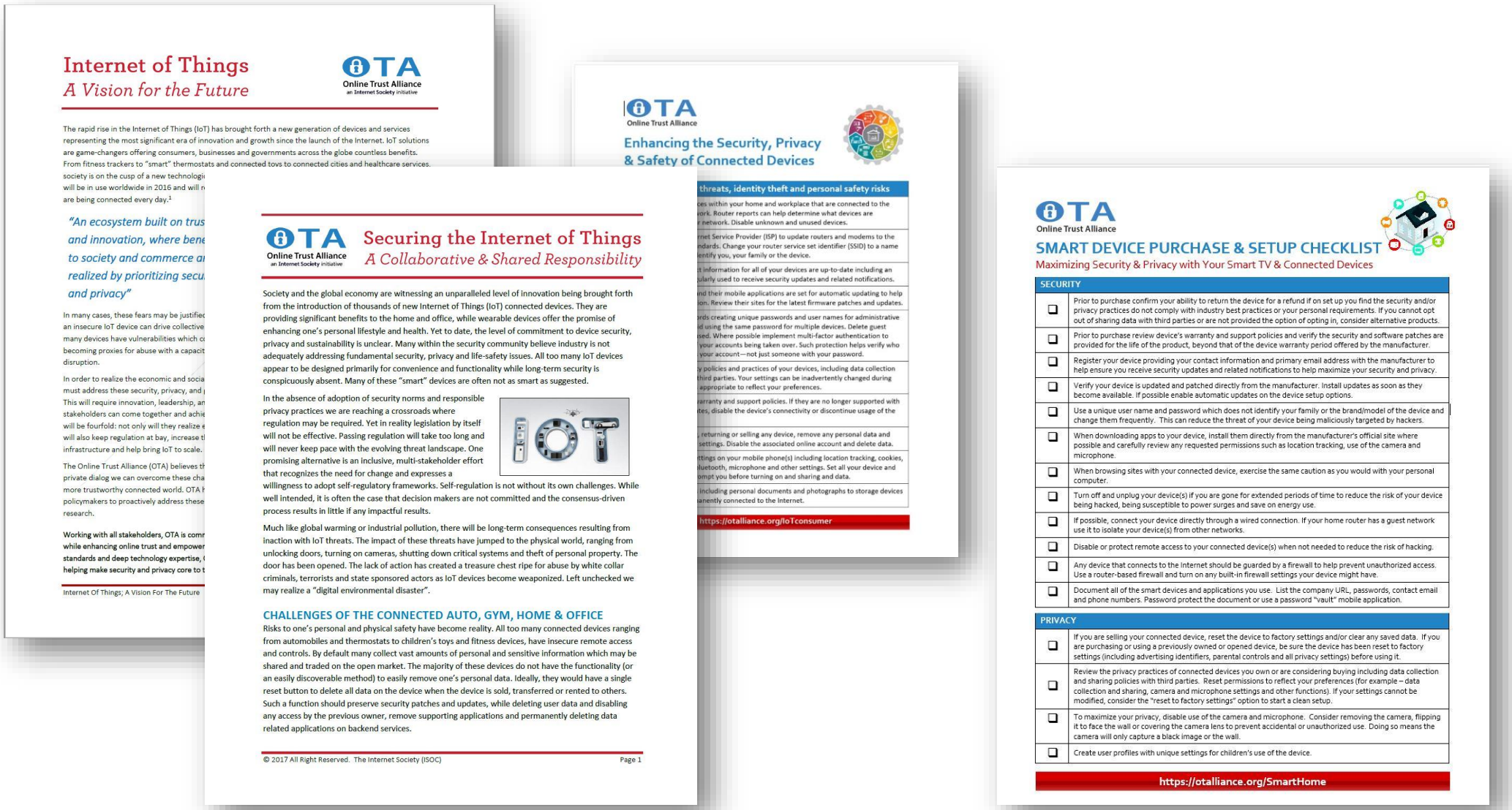
- **Inward Security**
  - Focus on potential harms to the health, safety, and privacy of device users and their property stemming from compromised IoT devices and systems
- **Outward Security**
  - Focus on potential harms that compromised devices and systems can inflict on the Internet and other users

Online Trust Alliance IoT Security & Privacy Trust Framework

- Measureable principles vs. standards development
- Consumer grade devices (home, office and wearables)
- Address known vulnerabilities and IoT threats
- Actionable and vendor neutral



Online Trust Alliance IoT Security Resources



Internet of Things
A Vision for the Future

Online Trust Alliance
an Internet Society initiative

The rapid rise in the Internet of Things (IoT) has brought forth a new generation of devices and services representing the most significant era of innovation and growth since the launch of the Internet. IoT solutions are game-changers offering consumers, businesses and governments across the globe countless benefits. From fitness trackers to "smart" thermostats and connected toys to connected cities and healthcare services, society is on the cusp of a new technologi
will be in use worldwide in 2016 and will
are being connected every day.[1]

*"An ecosystem built on trus
and innovation, where bene
to society and commerce a
realized by prioritizing secu
and privacy"*

In many cases, these fears may be justifie
an insecure IoT device can drive collective
many devices have vulnerabilities which c
becoming proxies for abuse with a capacit
disruption.

In order to realize the economic and socia
must address these security, privacy, and
This will require innovation, leadership, an
stakeholders can come together and achie
will be fourfold: not only will they realize
will also keep regulation at bay, increase t
infrastructure and help bring IoT to scale.

The Online Trust Alliance (OTA) believes th
private dialog we can overcome these cha
more trustworthy connected world. OTA h
policymakers to proactively address these
research.

**Working with all stakeholders, OTA is comm
while enhancing online trust and empower
standards and deep technology expertise,
helping make security and privacy core to t**

Internet Of Things; A Vision For The Future

Enhancing the Security, Privacy & Safety of Connected Devices

Online Trust Alliance

threats, identity theft and personal safety risks

ces within your home and workplace that are connected to the ork. Router reports can help determine what devices are network. Disable unknown and unused devices.

rnet Service Provider (ISP) to update routers and modems to the ndards. Change your router service set identifier (SSID) to a name entify you, your family or the device.

t information for all of your devices are up-to-date including an ularly used to receive security updates and related notifications.

nd their mobile applications are set for automatic updating to help on. Review their sites for the latest firmware patches and updates.

rds creating unique passwords and user names for administrative d using the same password for multiple devices. Delete guest sed. Where possible implement multi-factor authentication to your accounts being taken over. Such protection helps verify who your account—not just someone with your password.

y policies and practices of your devices, including data collection hird parties. Your settings can be inadvertently changed during appropriate to reflect your preferences.

arranty and support policies. If they are no longer supported with tes, disable the device's connectivity or discontinue usage of the

returning or selling any device, remove any personal data and settings. Disable the associated online account and delete data.

ttings on your mobile phone(s) including location tracking, cookies, luetooth, microphone and other settings. Set all your device and ompt you before turning on and sharing and data.

including personal documents and photographs to storage devices anently connected to the Internet.

https://otalliance.org/IoTconsumer

Securing the Internet of Things
A Collaborative & Shared Responsibility

Online Trust Alliance
an Internet Society initiative

Society and the global economy are witnessing an unparalleled level of innovation being brought forth from the introduction of thousands of new Internet of Things (IoT) connected devices. They are providing significant benefits to the home and office, while wearable devices offer the promise of enhancing one's personal lifestyle and health. Yet to date, the level of commitment to device security, privacy and sustainability is unclear. Many within the security community believe industry is not adequately addressing fundamental security, privacy and life-safety issues. All too many IoT devices appear to be designed primarily for convenience and functionality while long-term security is conspicuously absent. Many of these "smart" devices are often not as smart as suggested.

In the absence of adoption of security norms and responsible privacy practices we are reaching a crossroads where regulation may be required. Yet in reality legislation by itself will not be effective. Passing regulation will take too long and will never keep pace with the evolving threat landscape. One promising alternative is an inclusive, multi-stakeholder effort that recognizes the need for change and expresses a willingness to adopt self-regulatory frameworks. Self-regulation is not without its own challenges. While well intended, it is often the case that decision makers are not committed and the consensus-driven process results in little if any impactful results.

Much like global warming or industrial pollution, there will be long-term consequences resulting from inaction with IoT threats. The impact of these threats have jumped to the physical world, ranging from unlocking doors, turning on cameras, shutting down critical systems and theft of personal property. The door has been opened. The lack of action has created a treasure chest ripe for abuse by white collar criminals, terrorists and state sponsored actors as IoT devices become weaponized. Left unchecked we may realize a "digital environmental disaster".

CHALLENGES OF THE CONNECTED AUTO, GYM, HOME & OFFICE

Risks to one's personal and physical safety have become reality. All too many connected devices ranging from automobiles and thermostats to children's toys and fitness devices, have insecure remote access and controls. By default many collect vast amounts of personal and sensitive information which may be shared and traded on the open market. The majority of these devices do not have the functionality (or an easily discoverable method) to easily remove one's personal data. Ideally, they would have a single reset button to delete all data on the device when the device is sold, transferred or rented to others. Such a function should preserve security patches and updates, while deleting user data and disabling any access by the previous owner, remove supporting applications and permanently deleting data related applications on backend services.

 Page 1

SMART DEVICE PURCHASE & SETUP CHECKLIST

Online Trust Alliance

Maximizing Security & Privacy with Your Smart TV & Connected Devices

SECURITY	
❑	Prior to purchase confirm your ability to return the device for a refund if on set up you find the security and/or privacy practices do not comply with industry best practices or your personal requirements. If you cannot opt out of sharing data with third parties or are not provided the option of opting in, consider alternative products.
❑	Prior to purchase review device's warranty and support policies and verify the security and software patches are provided for the life of the product, beyond that of the device warranty period offered by the manufacturer.
❑	Register your device providing your contact information and primary email address with the manufacturer to help ensure you receive security updates and related notifications to help maximize your security and privacy.
❑	Verify your device is updated and patched directly from the manufacturer. Install updates as soon as they become available. If possible enable automatic updates on the device setup options.
❑	Use a unique user name and password which does not identify your family or the brand/model of the device and change them frequently. This can reduce the threat of your device being maliciously targeted by hackers.
❑	When downloading apps to your device, install them directly from the manufacturer's official site where possible and carefully review any requested permissions such as location tracking, use of the camera and microphone.
❑	When browsing sites with your connected device, exercise the same caution as you would with your personal computer.
❑	Turn off and unplug your device(s) if you are gone for extended periods of time to reduce the risk of your device being hacked, being susceptible to power surges and save on energy use.
❑	If possible, connect your device directly through a wired connection. If your home router has a guest network use it to isolate your device(s) from other networks.
❑	Disable or protect remote access to your connected device(s) when not needed to reduce the risk of hacking.
❑	Any device that connects to the Internet should be guarded by a firewall to help prevent unauthorized access. Use a router-based firewall and turn on any built-in firewall settings your device might have.
❑	Document all of the smart devices and applications you use. List the company URL, passwords, contact email and phone numbers. Password protect the document or use a password "vault" mobile application.

PRIVACY	
❑	If you are selling your connected device, reset the device to factory settings and/or clear any saved data. If you are purchasing or using a previously owned or opened device, be sure the device has been reset to factory settings (including advertising identifiers, parental controls and all privacy settings) before using it.
❑	Review the privacy practices of connected devices you own or are considering buying including data collection and sharing policies with third parties. Reset permissions to reflect your preferences (for example – data collection and sharing, camera and microphone settings and other functions). If your settings cannot be modified, consider the "reset to factory settings" option to start a clean setup.
❑	To maximize your privacy, disable use of the camera and microphone. Consider removing the camera, flipping it to face the wall or covering the camera lens to prevent accidental or unauthorized use. Doing so means the camera will only capture a black image or the wall.
❑	Create user profiles with unique settings for children's use of the device.

https://otalliance.org/SmartHome

ISOC “IoT Trust by Design” Campaign

• 1

- Work with manufacturers and suppliers to **adopt and implement the OTA IoT Trust Framework**

• 2

- **Mobilize consumers to drive demand** for security and privacy capabilities as a market differentiator

• 3

- Encourage policy and regulations to push for better security and privacy features in IoT

Activity highlights

- **OTA IoT Trust Framework implementation**
- Best practices and toolkits
- Implementation guide
- Training for ISOC and community

Research
- Paper on IoT Security for Policymakers
- Policy research: mapping the IoT policy/regulatory landscape
- Economic study on IoT security externalities
- Study on “consumer grade” IoT markets, to better understand manufacturing trends and consumer behaviour

Global, regional and local partnerships
- Security-minded IoT alliances
- Certification organizations
- Civil society organizations
- Organizations that review consumer products
- Internet Society community

Outreach to policy makers
- Regional engagement in strategic countries
- Global and regional events
- Workshops and capacity building
- Thought pieces and articles