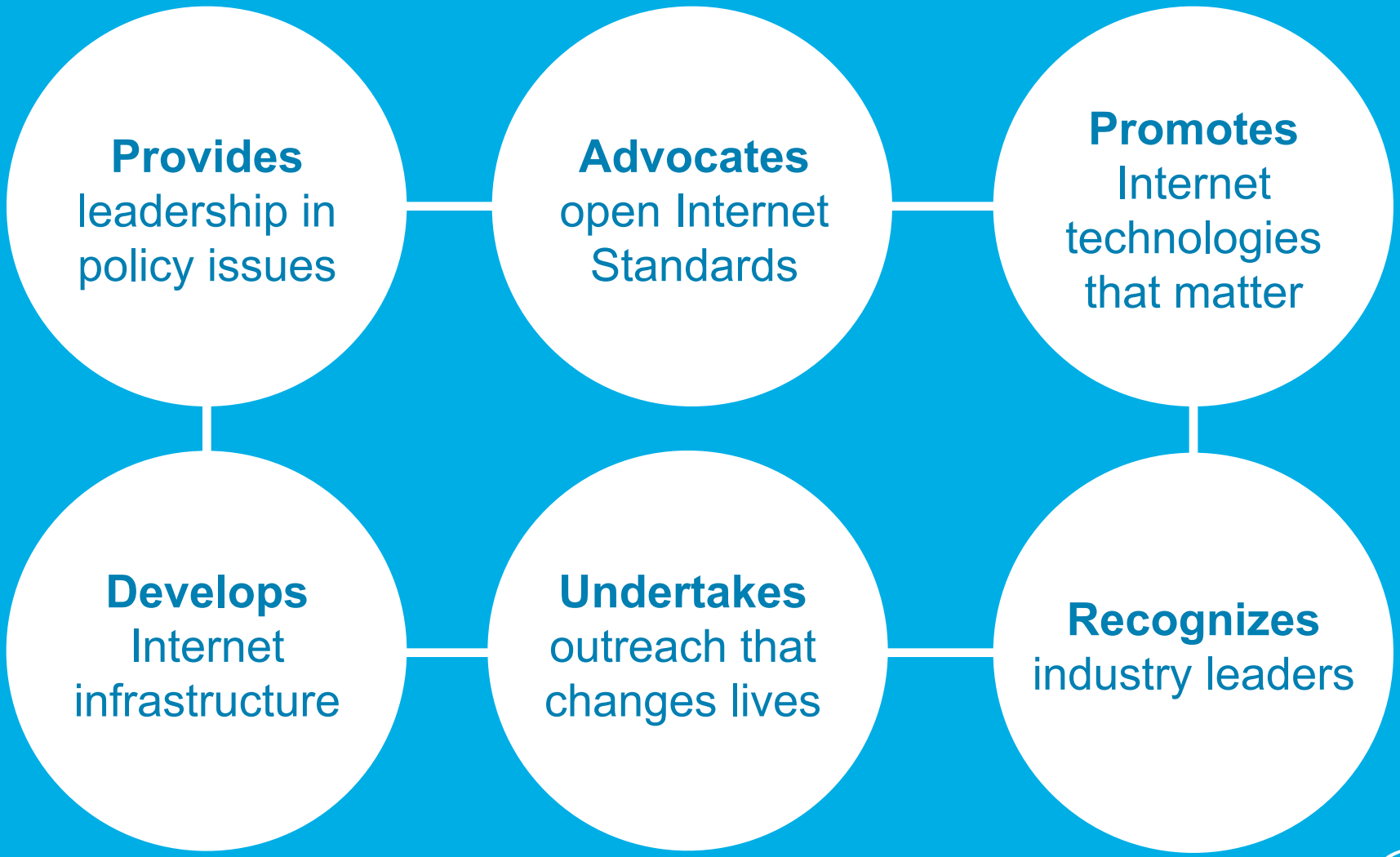
Privacy and Security in the IoT era

Our Mission

To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world.

The Internet Society at Work



What is the ‘Internet of Things’?

IoT broadly refers to the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be “computers”

The Internet of Things today

- Gartner estimates that there will be 6.4 billion connected things in use worldwide in 2016, up 30% from 2015
- This year, 5.5 million new things will get connected everyday
- Asia-Pacific leads in IoT development, accounting for 40% of worldwide IoT spending in 2015, and capturing more than 50% of the revenue from IoT—a trend that is expected to continue until 2020 (IDC)

Source: crn.com

…and tomorrow

Source: tech.eu

- More than half of major new business processes and systems will incorporate some element of IoT by 2020 (Gartner)
- The IoT market would evolve from its current focus of connecting devices to tapping the data collected by these devices (Frost & Sullivan)
- Mass deployment of near-identical connected devices, combined with the convergence of operational and information technology, opens the door for more vulnerabilities and attacks that cause greater impact

Internet Society

Why should we care?

- The IoT era would represent how we are likely to interact and engage with —and how we are impacted by--the Internet in our everyday lives
- The ‘smart objects’ will generate, exchange, and consume data, often with minimal human intervention
- It can represent a shift from an ‘active’ engagement to a ‘passive’ engagement with the Internet

Source: iotsecurityevent.com

What this means for our Privacy & Security

Increased centralisation of data

IoT represents a large network of sensor-enabled devices designed to collect data

Compared with our smartphones, tablets and laptops, IoT devices will be able to collect much more specific information about us, more pervasively

Much of this data can be sent to the ‘cloud’, shared with other devices, and may be accessed by other people

Increased third party mediation

Connectivity in many IoT devices will be ‘invisible’ and embedded in things that are familiar to us, and may thus give us a false sense of security

IoT devices frequently have no user interface that can tell us what data will be collected about us, how it will be used, and ask us if we agree to it

Many will also be designed to perform very specific tasks, and may not be able to detect and alert users of a security problem

Growing diversity of non-human agents

More and more day-to-day decisions will be made using algorithms

Algorithms will increasingly be adaptive—capable of autonomy and behaving in ways that undermine human agency

This can pose further challenges to our awareness of and control over what our devices gather and share about us

How will it affect our security?

Many IoT devices will be:

- **Deployed on a massive scale**
  - Having a lot more things connected to the Internet means a lot more possibilities for attack
- **Identical, or almost identical**
  - This means that one security threat can affect all devices of the same make and model
- **Designed to be in use for many, many years—and not designed to be 'upgradable'**
  - This makes them always vulnerable to new, evolving threats
- **Designed to do very specific tasks**
  - They may not be able to detect and alert users of a security problem
- **Built by small firms and individuals**
  - They may or may not apply industry best practices on security

Some security questions

- **Good design practices**
  - What are the best practices available for engineers and developers to design more secure IoT devices, and how do we ensure that these are implemented?
- **Cost vs. Security Trade-Offs**
  - How do we motivate device manufacturers and designers to make devices more secure, and to take responsibility for any negative impacts of their security decisions?
- **Shared responsibility**
  - How can shared responsibility and collaboration for IoT security be encouraged across stakeholders
- **Regulation**
  - Should device manufacturers be penalized for selling software or hardware with known or unknown security flaws?
  - How might product liability and consumer protection laws be adapted to cover any negative externalities related to the IoT?

Internet Society

Using IoT to solve development goals …and what this means for online privacy and security

The Future of Security is Collaborative

Internet Society

Preserving opportunities and building confidence

Traditional approaches to security were mainly concerned with external and internal threats, and the impact they may have on one's own assets

The Internet enables opportunities, for human, social and economic development on a global scale –this can only be realised if users trust the Internet enough to use it for their needs and innovations

The objective of security is to foster confidence in the Internet, rather than simply to prevent perceived harm

Collective responsibility

As networks are interconnected and interdependent, one stakeholder acting alone can make little difference, even in protecting its own resources

Internet security depends not only on how well participants manage security risks they face, but also, how they manage security risks that they may pose to others

Security solutions that are fully integrated with rights and the open Internet

Any security solution is likely to have a positive or negative effect on the Internet's operation and development, as well as user's rights and expectations

It is crucial that these solutions do not degrade the Internet's fundamental properties--its integrity, accessibility and global reach—which have made it such a valuable global resource

Security solutions that are grounded in experience and evolutionary in outlook

Security solutions need to be flexible enough to evolve over time, as technology changes and threats adapt

New efforts and solutions that build on “lessons-learned ” make the Internet more resilient to threats

A collection of incremental solutions may be more effective in practice than a grand design

Targeting the point of maximum impact

Security requires different players (within their different responsibilities and roles) to take action, closest to where the issues are occurring.

Typically, for greater effectiveness and efficiency, solutions should be defined and implemented by the smallest, lowest or least centralized competent community

…at the point in the system where they can have the most impact

Rethinking online trust

- Trust is the belief that someone will act in your interest even if they have the means to do otherwise—and many of our activities online are powered or monitored by third parties whose motivations may be incompatible with our privacy and security
- There is a gap between our expectations of trust based on real life and our interactions in the digital world, where we tend to trust unknown systems and entities who we haven't met and over whom we have no control
- Trust is always contextual—it is trusting someone to do or be able to do something specific, but perhaps not other things (e.g. trusting your bank, but not your neighbor, to have access to your bank account details)
- We tend to think of trust as a state—instead, we should think of it as a process that requires constant work to maintain

Thank You

Internet Society