Privacy and Security Aspects of IoT Solutions

Jonathan Brewer - NSRC

IOT and Privacy Issues

Universal Declaration of Human Rights article 12:
International Covenant on Civil and Political Rights article 17:

- No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honour and reputation.
- Everyone has the right to the protection of the law against such interference or attacks.

IOT and Privacy Issues

68/167 The right to privacy in the digital age

Resolution adopted by the General Assembly on 18 December 2013

"unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society"

"while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law"

IOT and Privacy Issues

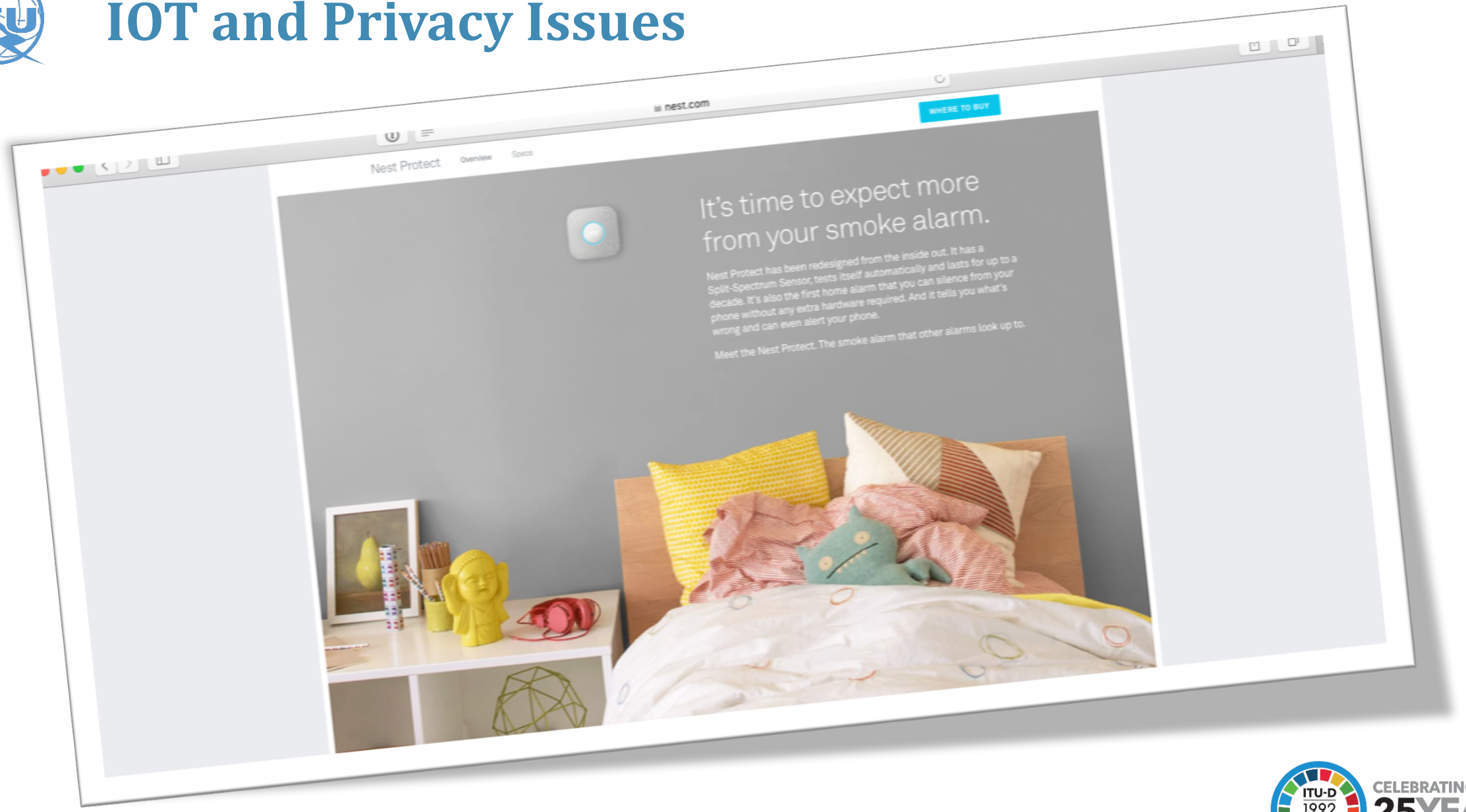
68/167 The right to privacy in the digital age

Resolution adopted by the General Assembly on 18 December 2013

"Calls upon all States: …to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law"

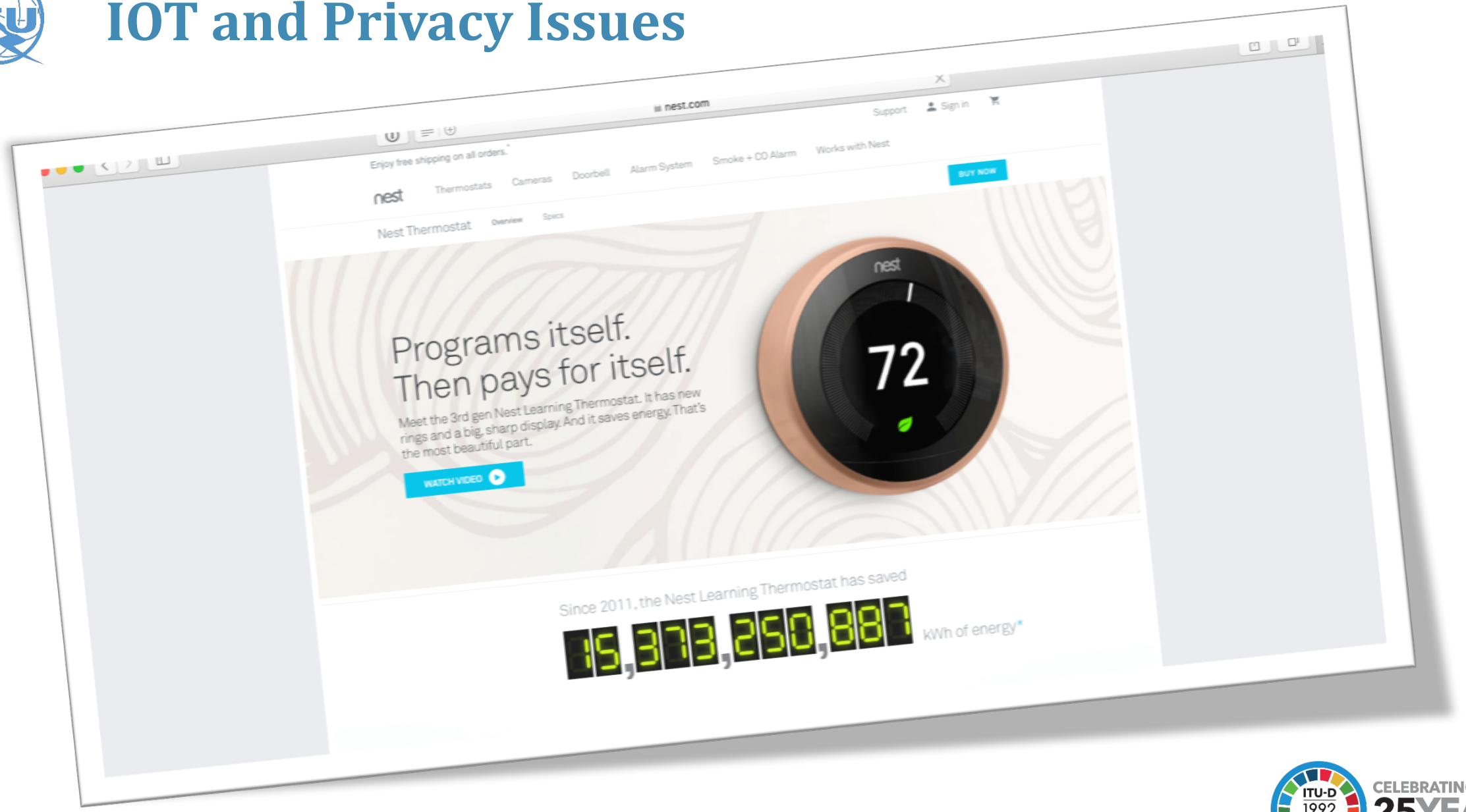
How can the IoT compromise our right to privacy?

IOT and Privacy Issues



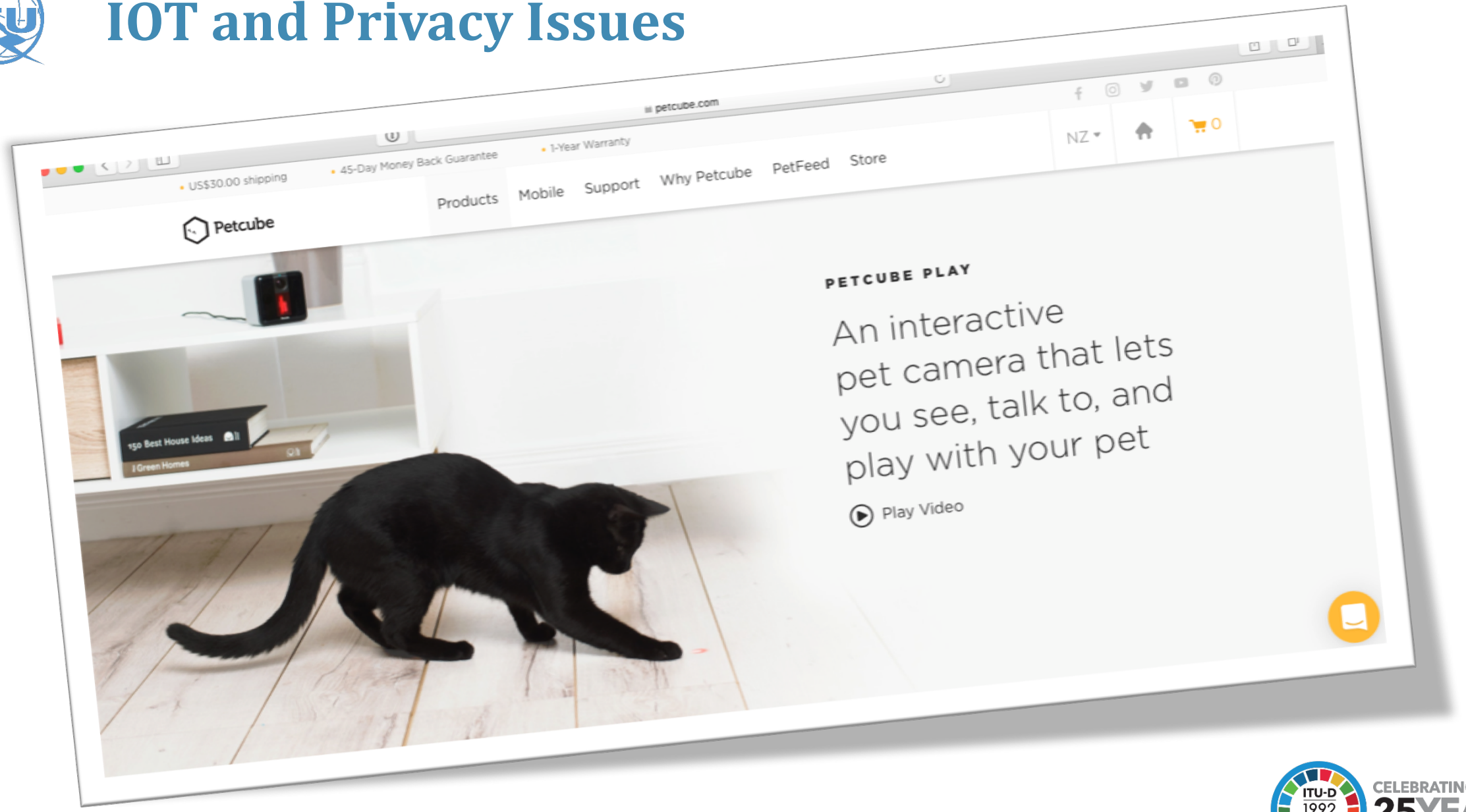
CELEBRATING 25 YEARS OF ACHIEVEMENTS

IOT and Privacy Issues



CELEBRATING 25 YEARS OF ACHIEVEMENTS

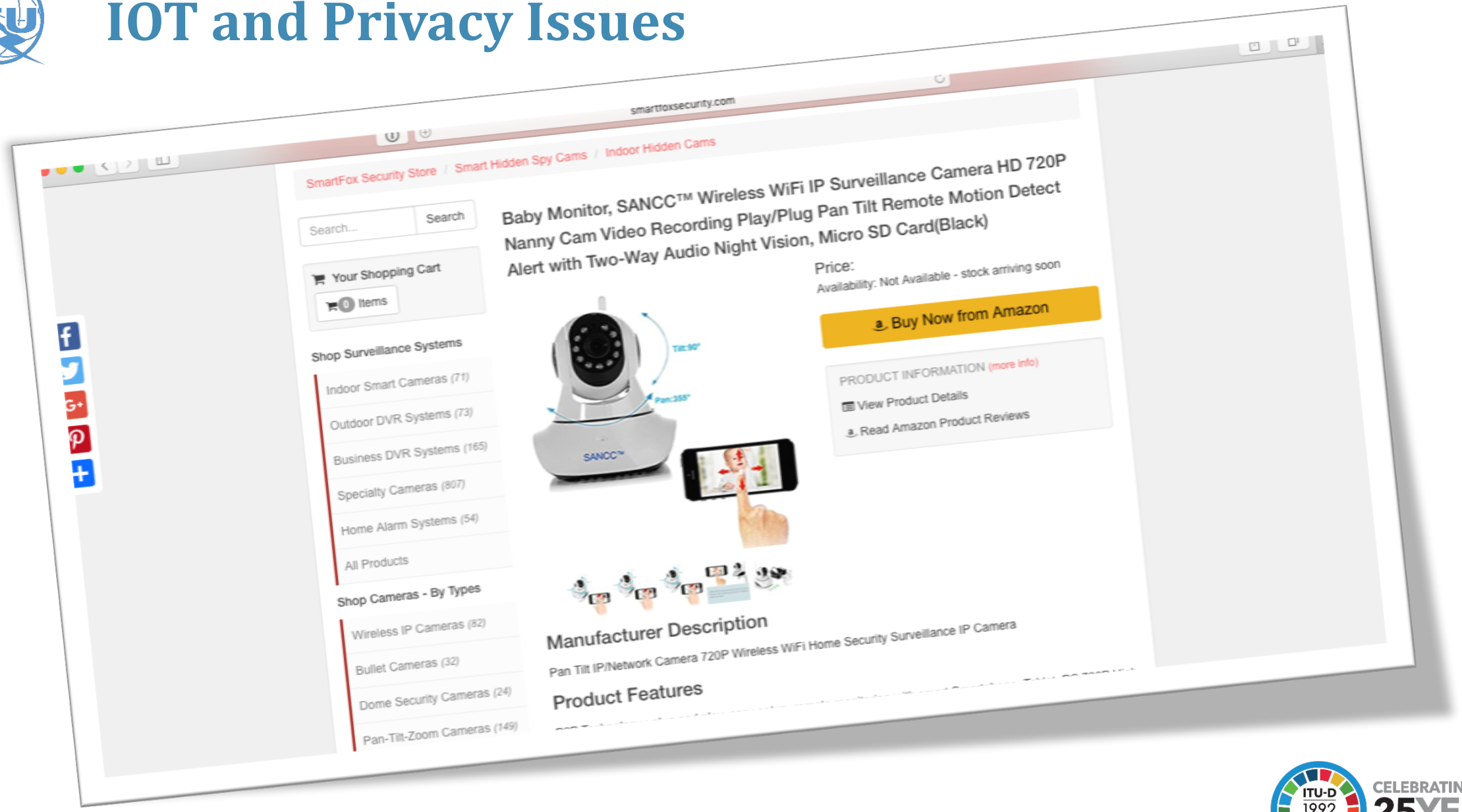
IOT and Privacy Issues



IOT and Privacy Issues

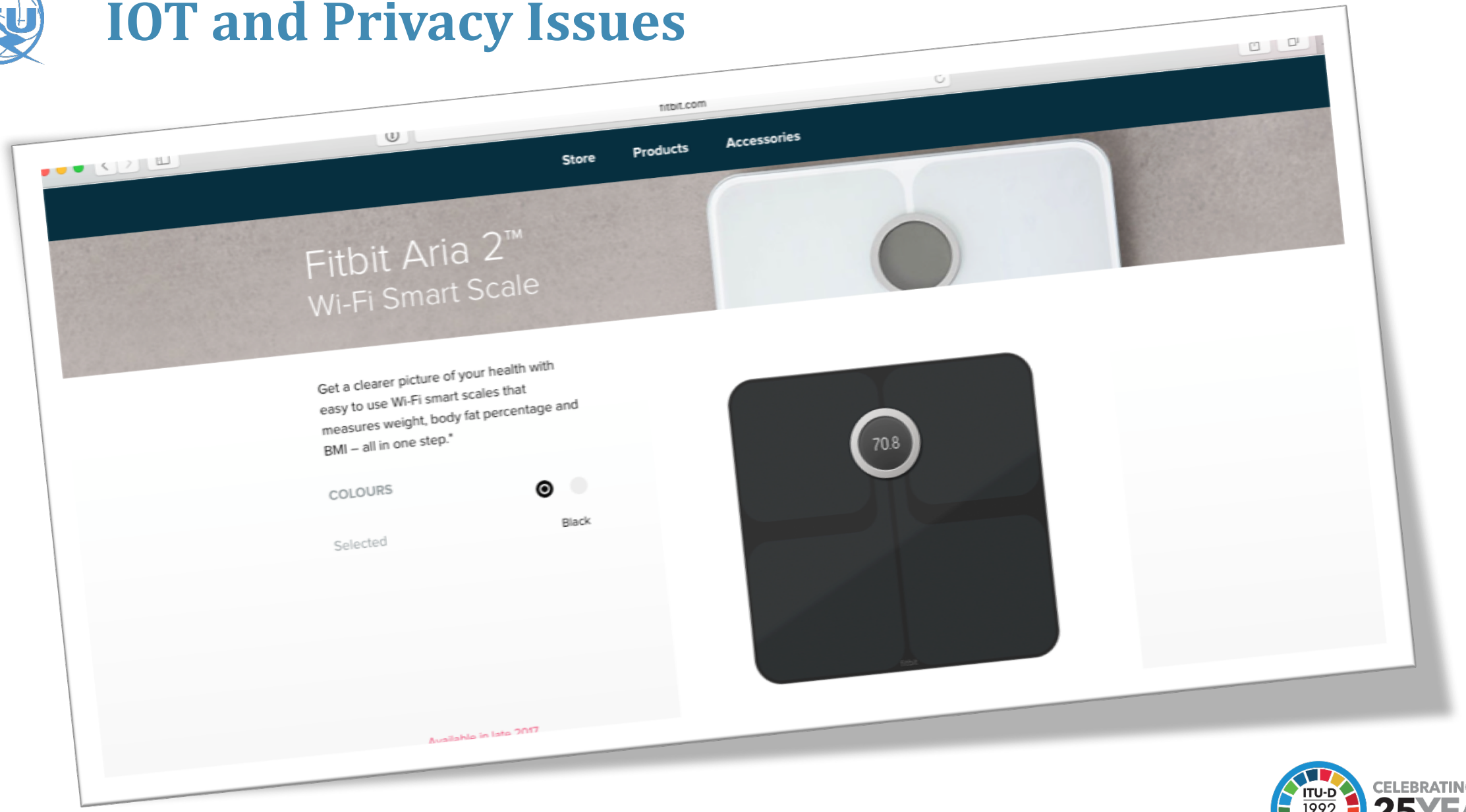
CELEBRATING 25 YEARS OF ACHIEVEMENTS

IOT and Privacy Issues



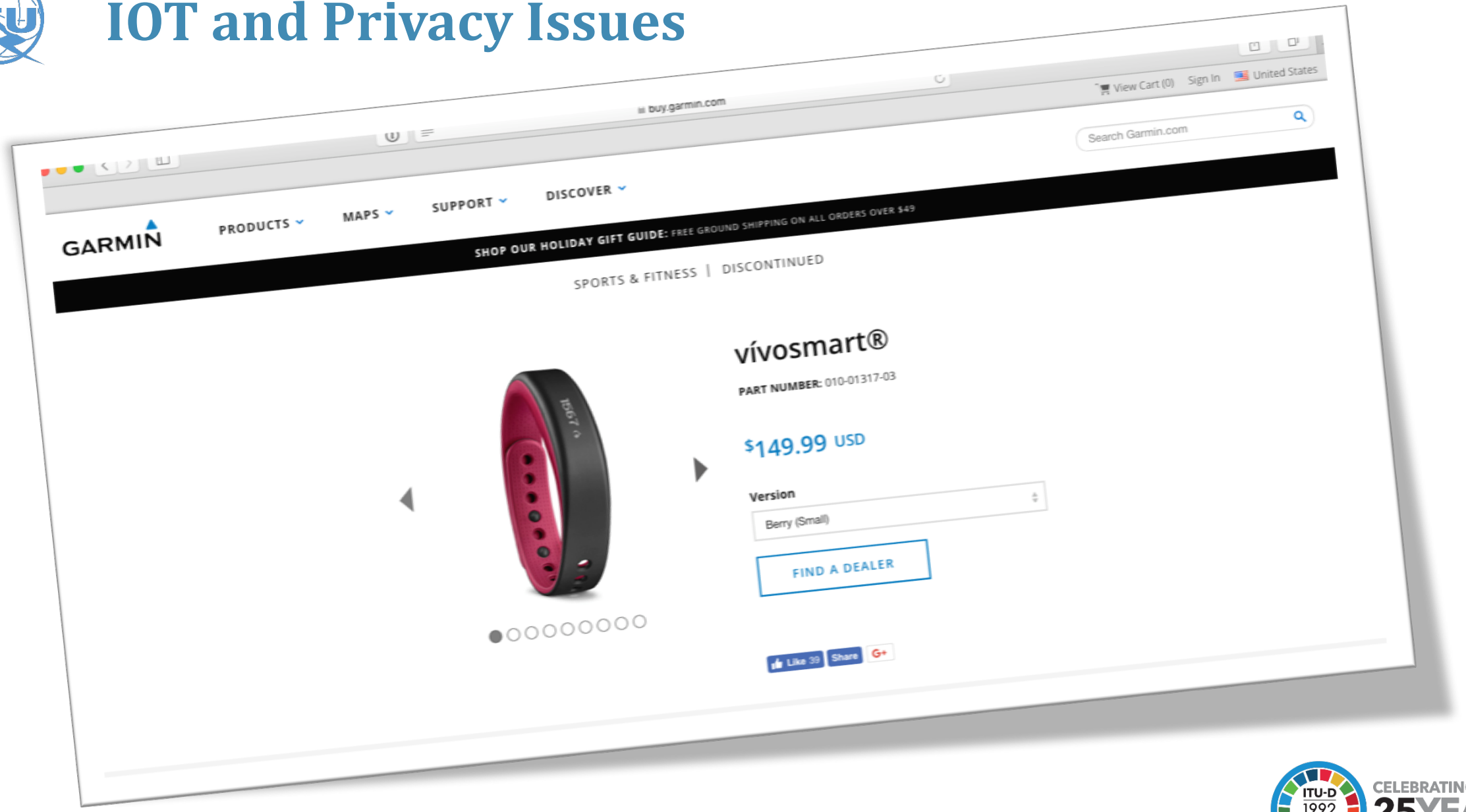
CELEBRATING 25 YEARS OF ACHIEVEMENTS

IOT and Privacy Issues



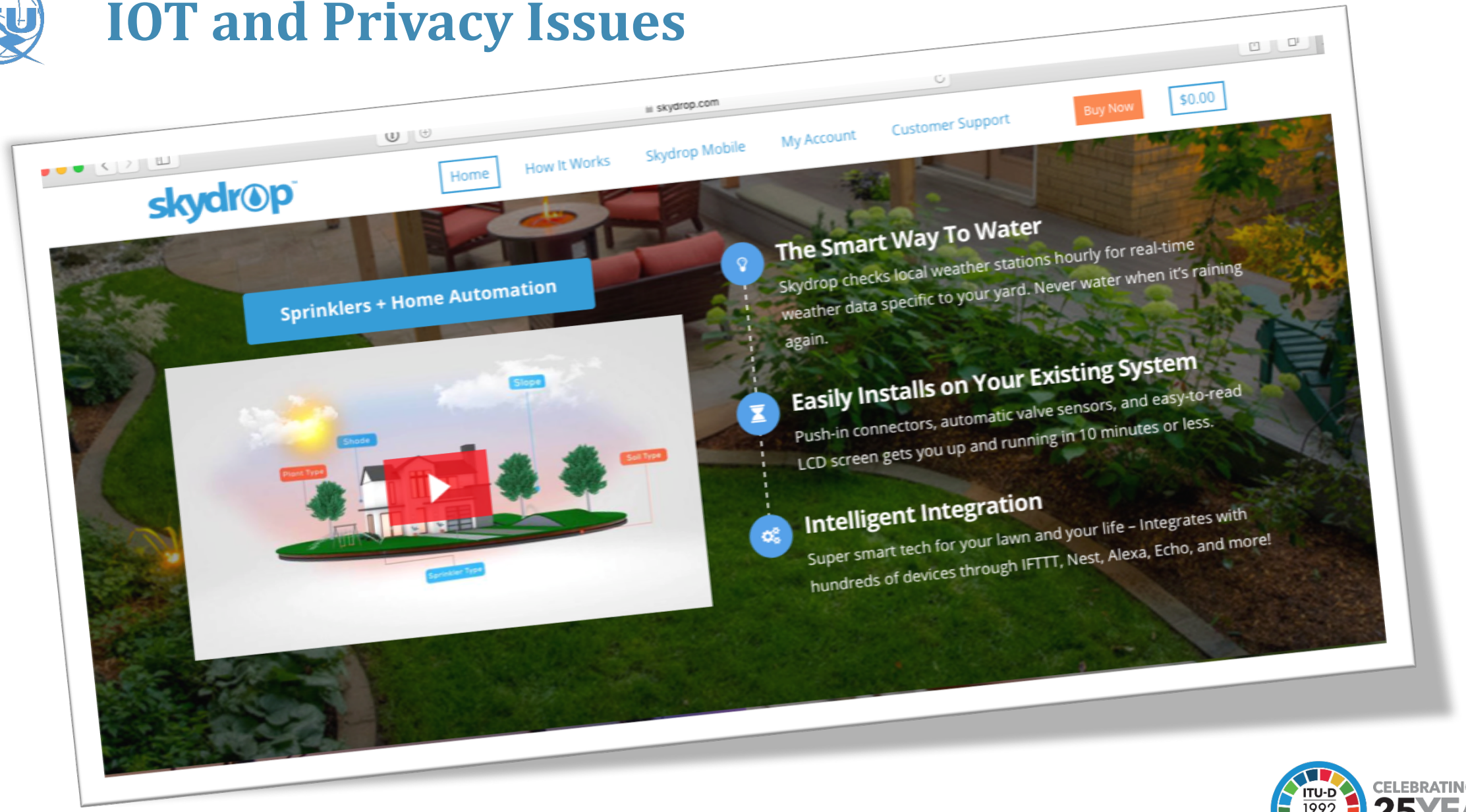
CELEBRATING 25 YEARS OF ACHIEVEMENTS

IOT and Privacy Issues



CELEBRATING 25 YEARS OF ACHIEVEMENTS

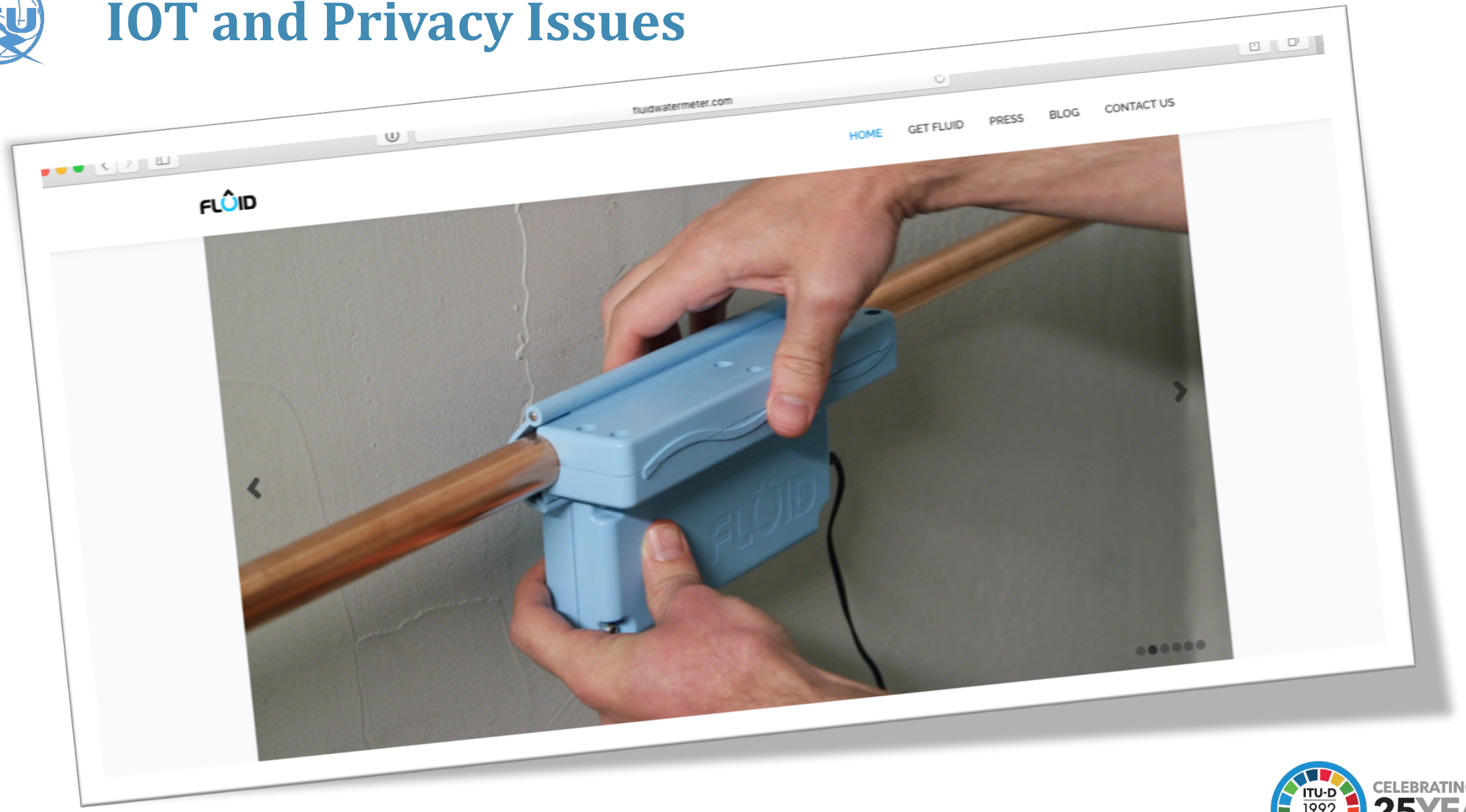
IOT and Privacy Issues



IOT and Privacy Issues

CELEBRATING 25 YEARS OF ACHIEVEMENTS

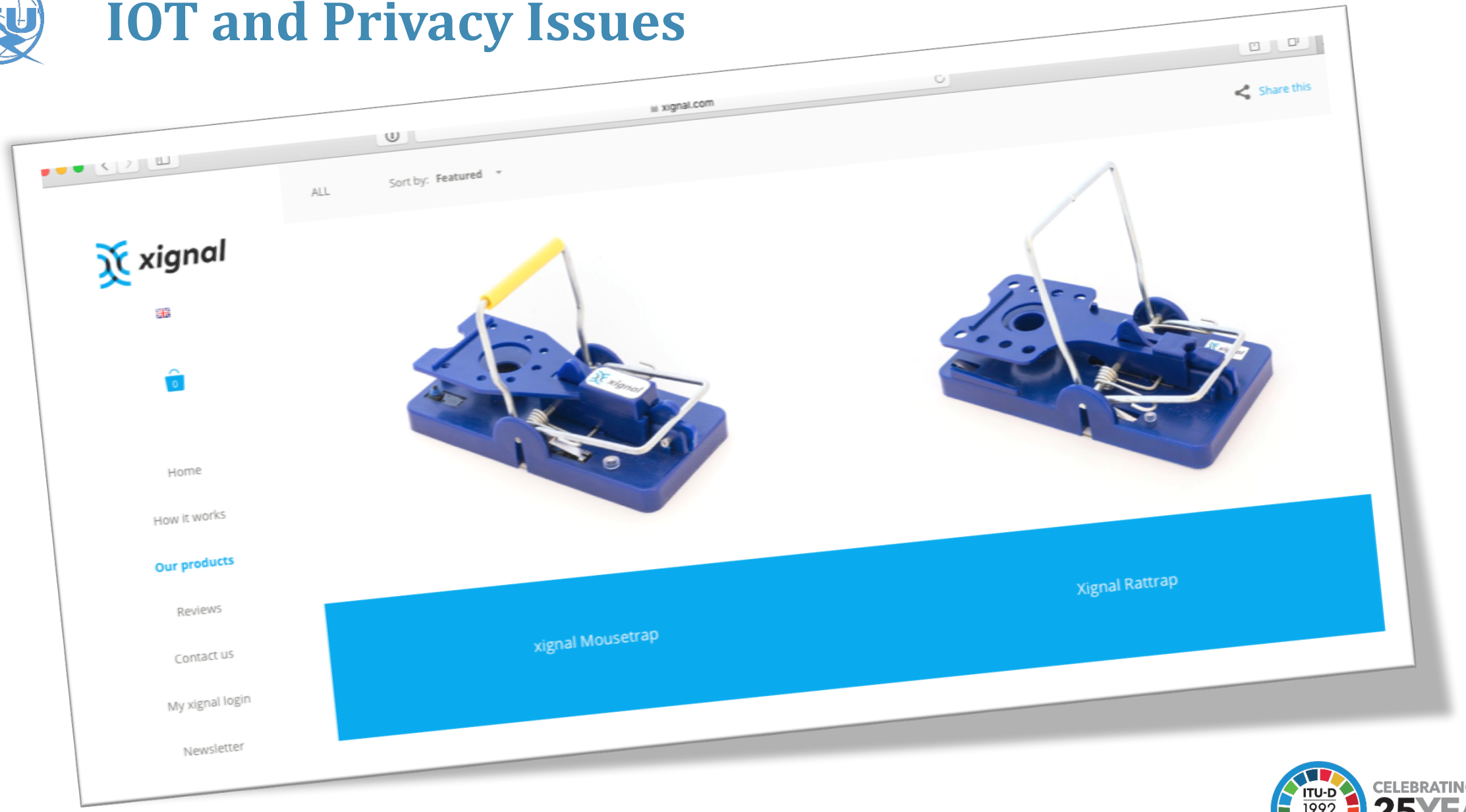
IOT and Privacy Issues



IOT and Privacy Issues

CELEBRATING 25 YEARS OF ACHIEVEMENTS

IOT and Privacy Issues



CELEBRATING 25 YEARS OF ACHIEVEMENTS

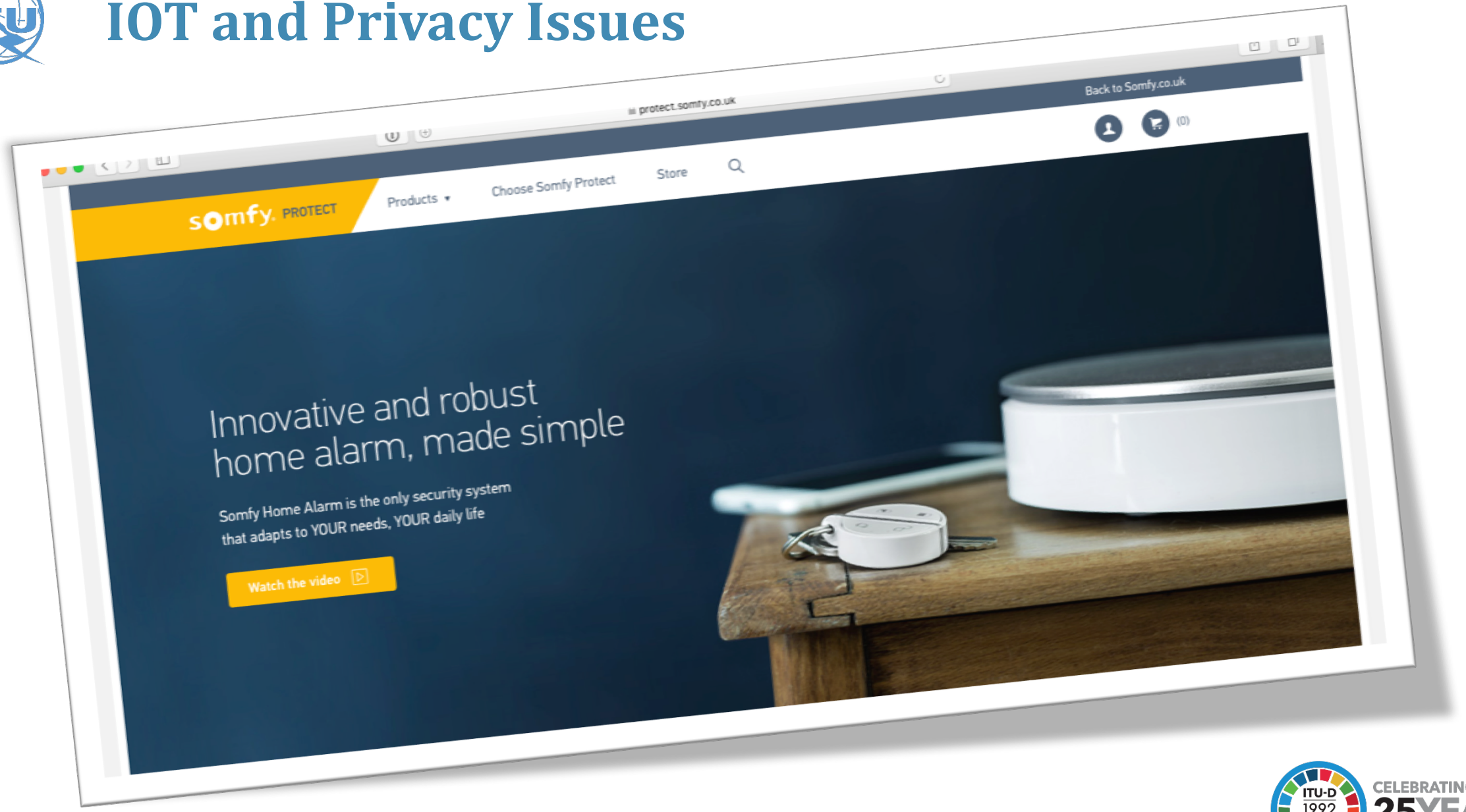
IOT and Privacy Issues

CELEBRATING 25 YEARS OF ACHIEVEMENTS

IOT and Privacy Issues

CELEBRATING 25 YEARS OF ACHIEVEMENTS

IOT and Privacy Issues



How can we prevent IoT from compromising our right to privacy?

IOT and Privacy Issues

OECD Privacy Principles

Collection Limitation	**Data Quality**
Purpose Specification	**Use Limitation**
Security Safeguards	**Openness**
Individual Participation	**Accountability**

IOT and Privacy Issues

OECD Privacy Principles: Collection Limitation

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

IOT and Privacy Issues

OECD Privacy Principles: Data Quality

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

IOT and Privacy Issues

OECD Privacy Principles: Purpose Specification

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

IOT and Privacy Issues

OECD Privacy Principles: Use Limitation

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

IOT and Privacy Issues

OECD Privacy Principles: Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

IOT and Privacy Issues

OECD Privacy Principles: Openness

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

IOT and Privacy Issues

OECD Privacy Principles: Individual Participation

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

IOT and Privacy Issues

OECD Privacy Principles: Accountability

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Privacy Requires Security

Prosperity Requires Security

Safety Requires Security

IOT and Security: Threat Modelling

What IoT assets are in use?

- Agriculture
- Enterprise & Government
- Home
- Industrial Production
- Smart City
- Transportation

IOT and Security: Threat Modelling

What Are IoT Attack Surfaces?

Ecosystem (General)	**Device Memory**	**Dev Physical Interfaces**	**Device Web Interface**
Device Firmware	**Dev Network Services**	**Administrative Interface**	**Local Data Storage**
Cloud Web Interface	**3rd Party Backend API**	**Update Mechanism**	**Mobile Application**
Vendor Backend API	**Ecosystem Communication**	**Network Traffic**	**Authentication**
Authorization	**Privacy**	**Hardware (Sensors)**	

https://www.owasp.org/

IOT and Security: Threat Modelling

What are IoT Vulnerabilities?

Username Enumeration	**Weak Passwords**	**Account Lockout**	**Unencrypted Services**
Two-Factor Authentication	**Poor Encryption**	**Updates Sent Without Encryption**	**Update Location Writable**
Denial of Service	**Removal of Storage Media**	**No Manual Update Mechanism**	**Missing Update Mechanism**
Firmware Version Display	**Firmware and Storage Extraction**	**Manipulating Code Execution Flow of Device**	**Obtaining Console Access**
Insecure 3rd Party Components			

https://www.owasp.org/

IOT and Security: Threat Modelling

- Characterizing Threats: STRIDE
  - Spoofing Identity
  - Tampering with Data
  - Repudiation
  - Information Disclosure
  - Denial of Service
  - Elevation of Privilege

https://www.owasp.org/

IOT and Security: Threat Modelling

- Classifying Threats: DREAD
  - Damage Potential
  - Reproducibility
  - Exploitability
  - Affected Users
  - Discoverability

https://www.owasp.org/

IOT and Security: Threat Examples

Smart City / Transportation

- Inflate Pedestrian Count = Slow City Traffic
- Disrupt Smart Motorway = Slow Highway Traffic
- Interfere with Parking Sensors = Keep Cars on the Road
- Spoof Infrastructure Faults = Occupy Maintenance Workers
- Fake Water Meter Readings = False Water Crisis & Restrictions

IOT and Security: Threat Examples

Industrial Production

- Interfere with Temperature Sensors: Excess AC Use
- Take Over Smart Lighting: Disrupt Production
- Interfere with Fire Sensors: Disrupt Production
- Falsify Smart Meter Readings: Utilities Fraud
- Compromise CCTV: Industrial Espionage

IOT and Security: Threat Examples

Enterprise & Government

- Hack Cloud Printing: Data Theft
- Compromise Manager Home Cameras: Blackmail
- Interfere with Fire Sensors: Close Office
- Falsify Smart Meter Readings: Utilities Fraud
- Compromise CCTV: Espionage

IOT and Security: Combating Threats

- Evaluate Every IoT Application
  - Consider STRIDE, DREAD, Vulnerabilities, Attack Surfaces
- Choose Secure IoT Protocols
  - nbIoT, LoRaWAN, LTE-M are designed with security
- Choose Secure IoT Platforms
  - Platforms must support Authentication, Access, Audit

Thank You

CELEBRATING 25 YEARS OF ACHIEVEMENTS