All Things Considered: An Analysis of IoT Devices on Home Networks

Deepak Kumar
University of Illinois

Kelly Shen
Stanford University

Benton Case
Stanford University

Deepali Garg
Avast Software

Galina Alperovich
Avast Software

Dmitry Kuznetsov
Avast Software

Rajarshi Gupta
Avast Software

Zakir Durumeric
Stanford University

Smart home devices attract hackers in their first five minutes online

‘World’s first Bluetooth hair straighteners’ can be easily hacked

Researchers demonstrate new ways to hack your stupidly complex smart home

'I'm in your baby's room': Nest cam hacks show risk of internet-connected devices

How one lightbulb could allow hackers to burgle your home

Security flaws in a popular smart home hub let hackers unlock front doors

We have little visibility into the devices consumers are putting into their homes

What does the home IoT ecosystem look like?

Avast Wi-Fi Inspector

Avast Wi-Fi Inspector

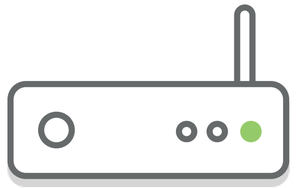
- Performs internal network scans and checks devices for weak security

Avast Wi-Fi Inspector

- Performs internal network scans and checks devices for weak security
  - Device identification
  - Weak default credentials
  - Vulnerability to known recent CVEs

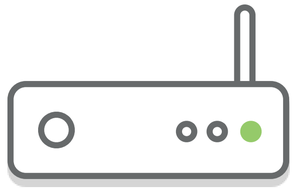
Avast Wi-Fi Inspector

Open Services



Avast Wi-Fi Inspector

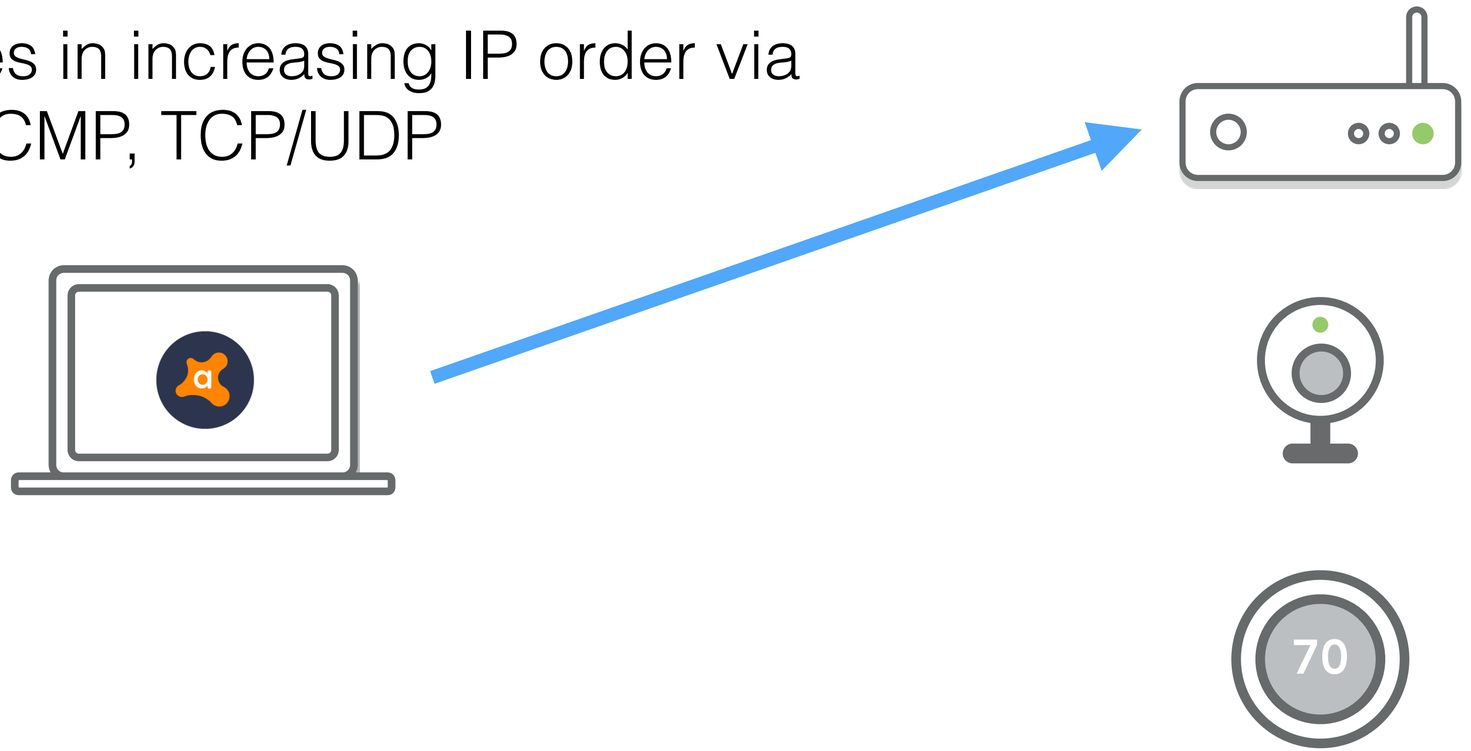
Probe devices in increasing IP order via ICMP, TCP/UDP



Open Services

Avast Wi-Fi Inspector

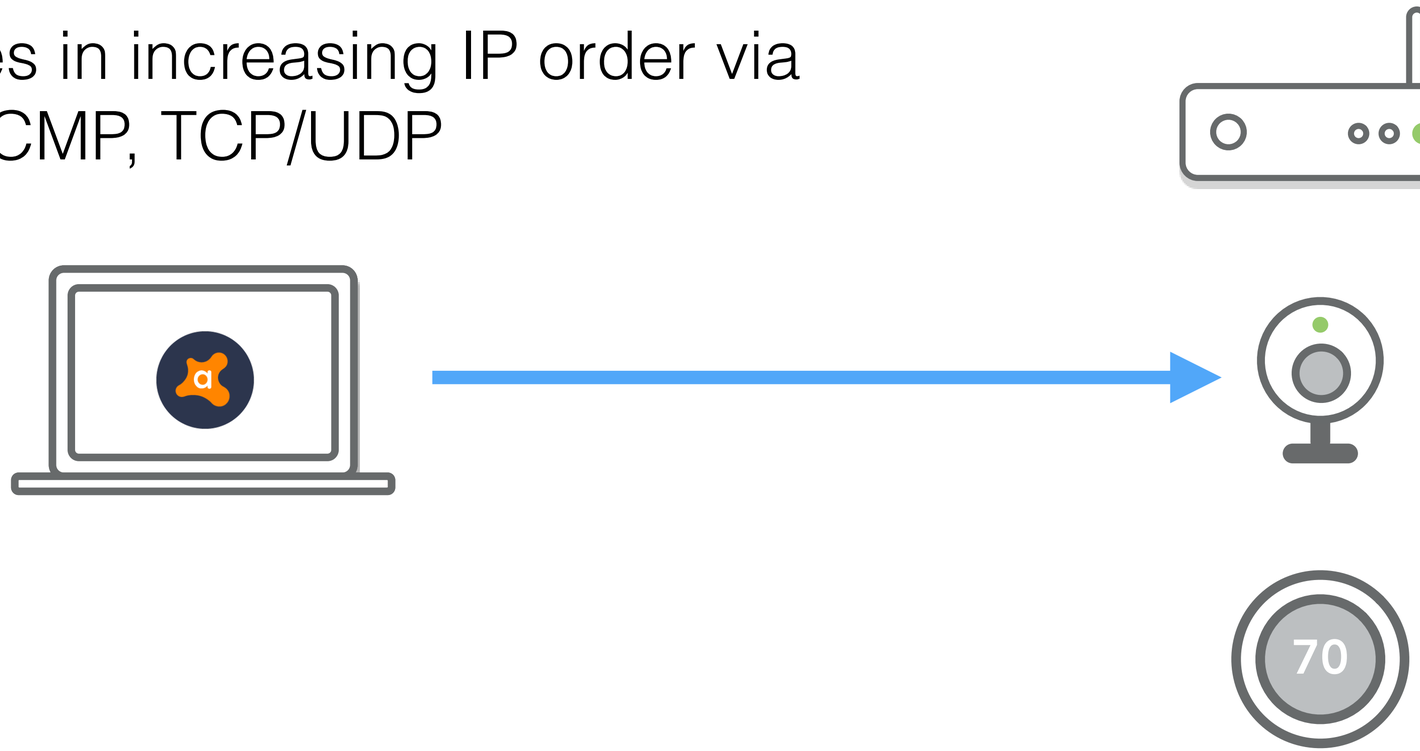
Probe devices in increasing IP order via ICMP, TCP/UDP



Open Services
80, 443, 23, 53

Avast Wi-Fi Inspector

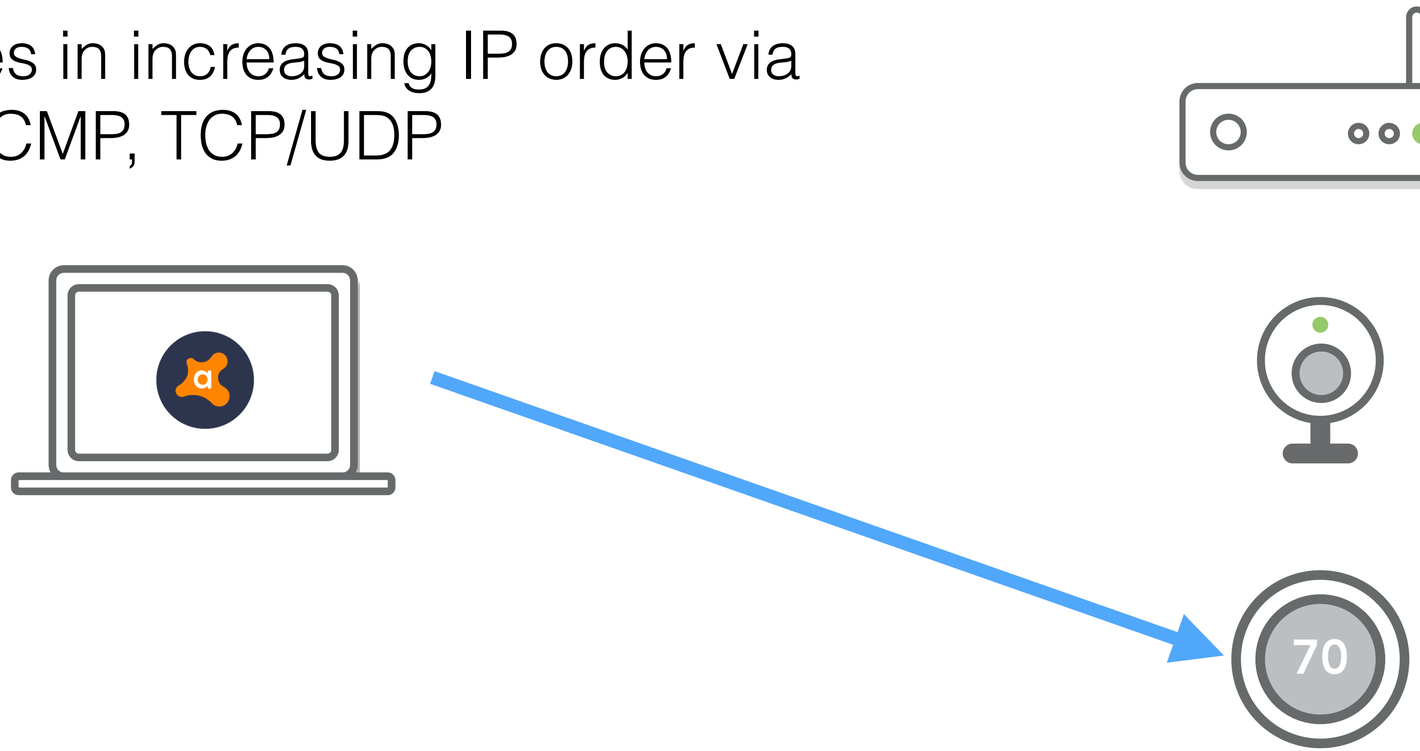
Probe devices in increasing IP order via ICMP, TCP/UDP



Open Services
80, 443, 23, 53
21, 22, 23

Avast Wi-Fi Inspector

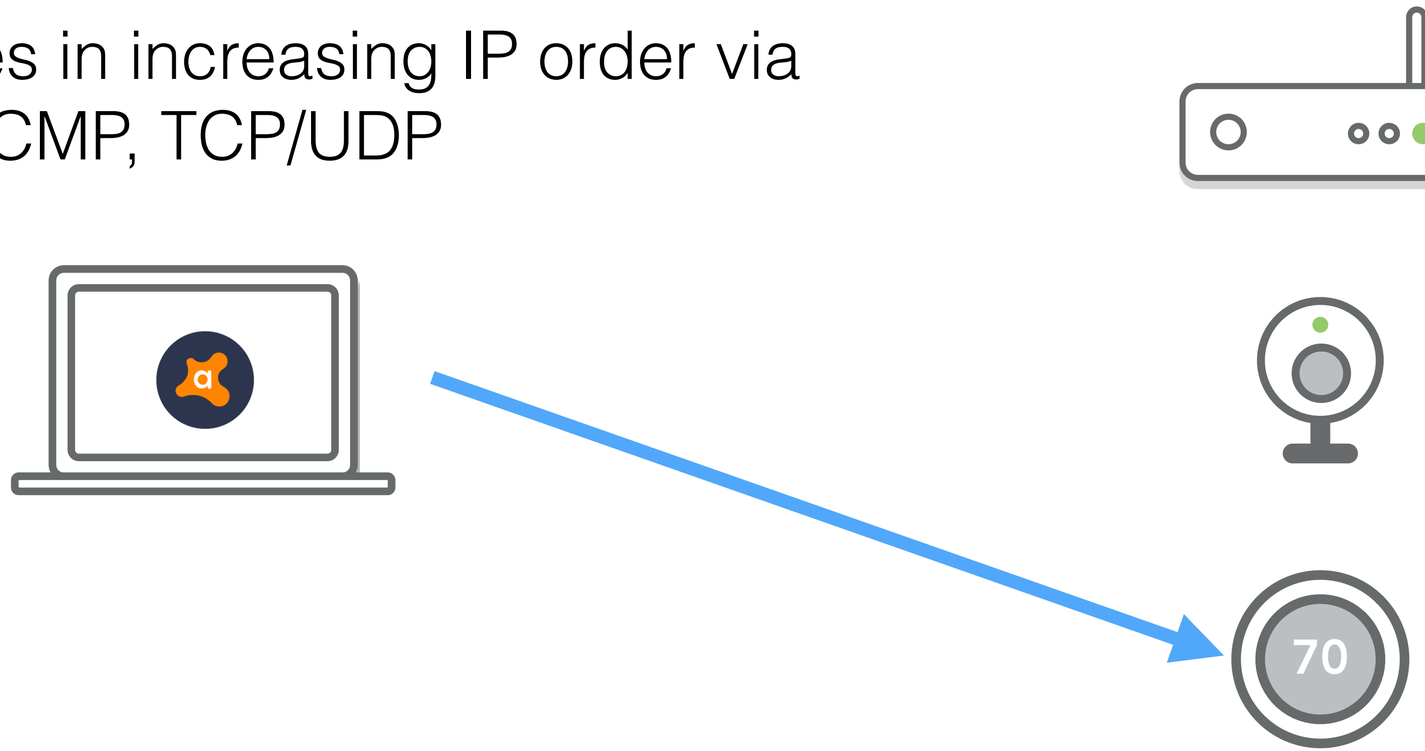
Probe devices in increasing IP order via ICMP, TCP/UDP



Open Services
80, 443, 23, 53
21, 22, 23
80, 443, 1900

Avast Wi-Fi Inspector

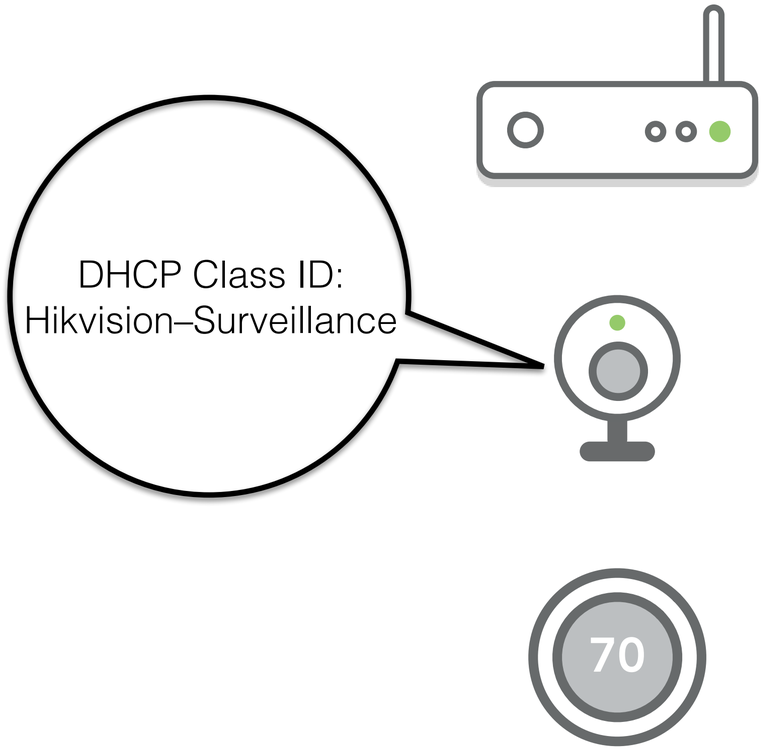
Probe devices in increasing IP order via ICMP, TCP/UDP



Open Services
80, 443, 23, 53
21, 22, 23
80, 443, 1900, 23

Avast Wi-Fi Inspector

Collects semantically rich broadcast/multicast traffic via DHCP, mDNS, UPnP



Open Services
80, 443, 23, 53
21, 22, 23
80, 443, 1900, 23

Avast Wi-Fi Inspector: DeviceID

- Determine device vendor, fit device into one of 14 device classes

Avast Wi-Fi Inspector: DeviceID Classes

Device Classes	
Computer	Router
Mobile Device	Wearable
Game Console	Home Automation
Storage	Surveillance
Work Appliance	Voice Assistant
Vehicle	Media/TV
Home Appliance	Generic IoT

Avast Wi-Fi Inspector: DeviceID Classes

Device Classes	
Computer	Router
Mobile Device	**Wearable**
Game Console	**Home Automation**
Storage	**Surveillance**
Work Appliance	**Voice Assistant**
Vehicle	**Media/TV**
Home Appliance	**Generic IoT**

Avast Wi-Fi Inspector: DeviceID

- Determine device vendor, fit device into one of 14 device classes
  - Network Rules (regex)

Network Rules

Protocol	Field	Pattern	Type
DHCP	Class ID	`(?i)SAMSUNG[- :_]Network[- :_]Printer`	Printer
mDNS	Name	`(?i)_nanoleaf(?:api|ms)?\._tcp\.local\.`	Lighting
UPnP	Device Type	`.*hub2.*`	IoT Hub
HTTP	Title	`(?i)Polycom - (?:SoundPoint IP )?(?:SoundStation IP )?`	VoIP Phone

Avast Wi-Fi Inspector: DeviceID

- Determine device vendor, fit device into one of 14 device classes
  - Network Rules (regex)
  - Supervised ML

Supervised ML

- Ensemble model that leverages several network features
- Trained on 500K devices from real world scans
  - 300K labels from network rules
  - 200K manually labeled
- Tested on a set of 1K manually labeled unseen devices

Machine Learning

Classifier	Coverage	Accuracy	F1
Network	0.89	0.96	0.79
UPnP	0.27	0.91	0.37
mDNS	0.05	0.94	0.25
HTTP	0.14	0.98	0.23
Supervised Ensemble	**0.92**	**0.96**	**0.8**

Ethical Considerations

- Avast only shared **aggregate** data to our team, aggregated by device manufacturer, region, and device type
- **No personally identifiable** data was shared with research team, including IP addresses of homes
- Scans in our dataset are all *user initiated,* never automated

Dataset

Network scans collected from
15.5 million homes, spanning
83 million devices across
11 geographic regions

What do home networks look like?

Homes w/ IoT Devices

Region	% Homes w/ IoT Device	Med. Devices per Home
North America	66.3%	7
Western Europe	53.5%	4
Oceania	49.2%	4
Central + South America	31.7%	4
East Asia	30.8%	3
Eastern Europe	25.2%	3
Southeast Asia	21.7%	4
Sub-Saharan Africa	19.7%	3
North Africa/Middle East	19.1%	3
Central Asia	17.3%	2
South Asia	8.7%	2

Homes w/ IoT Devices

Region	% Homes w/ IoT Device	Med. Devices per Home
North America	**66.3%**	**7**
Western Europe	**53.5%**	**4**
Oceania	**49.2%**	**4**
Central + South America	31.7%	4
East Asia	30.8%	3
Eastern Europe	25.2%	3
Southeast Asia	21.7%	4
Sub-Saharan Africa	19.7%	3
North Africa/Middle East	19.1%	3
Central Asia	17.3%	2
South Asia	8.7%	2

Homes w/ IoT Devices

Region	% Homes w/ IoT Device	Med. Devices per Home
North America	66.3%	7
Western Europe	53.5%	4
Oceania	49.2%	4
Central + South America	31.7%	4
East Asia	30.8%	3
Eastern Europe	25.2%	3
Southeast Asia	21.7%	4
Sub-Saharan Africa	19.7%	3
North Africa/Middle East	**19.1%**	**3**
Central Asia	**17.3%**	**2**
South Asia	**8.7%**	**2**

What is an IoT device?*

*empirically

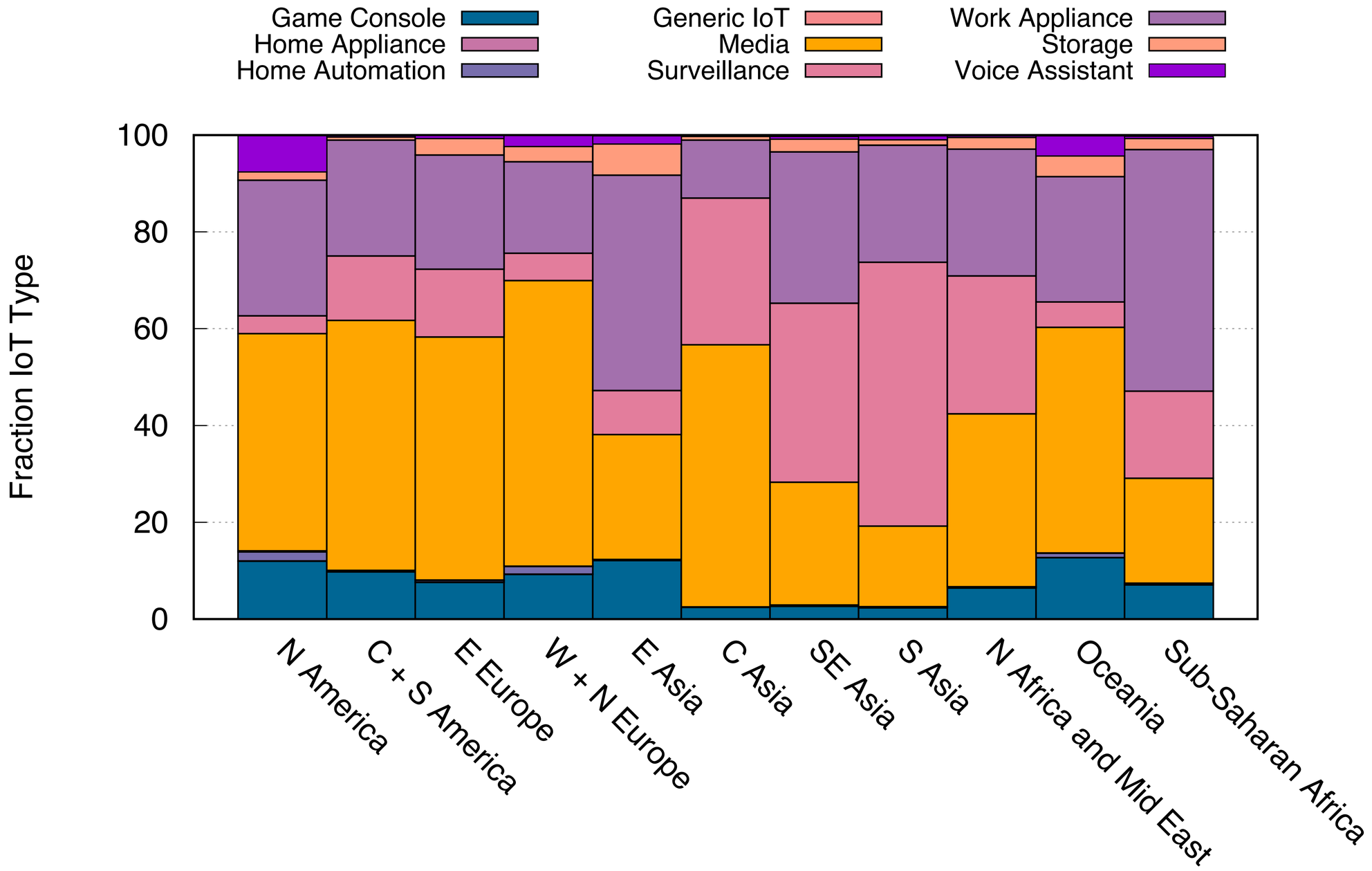
A Typical North American Home

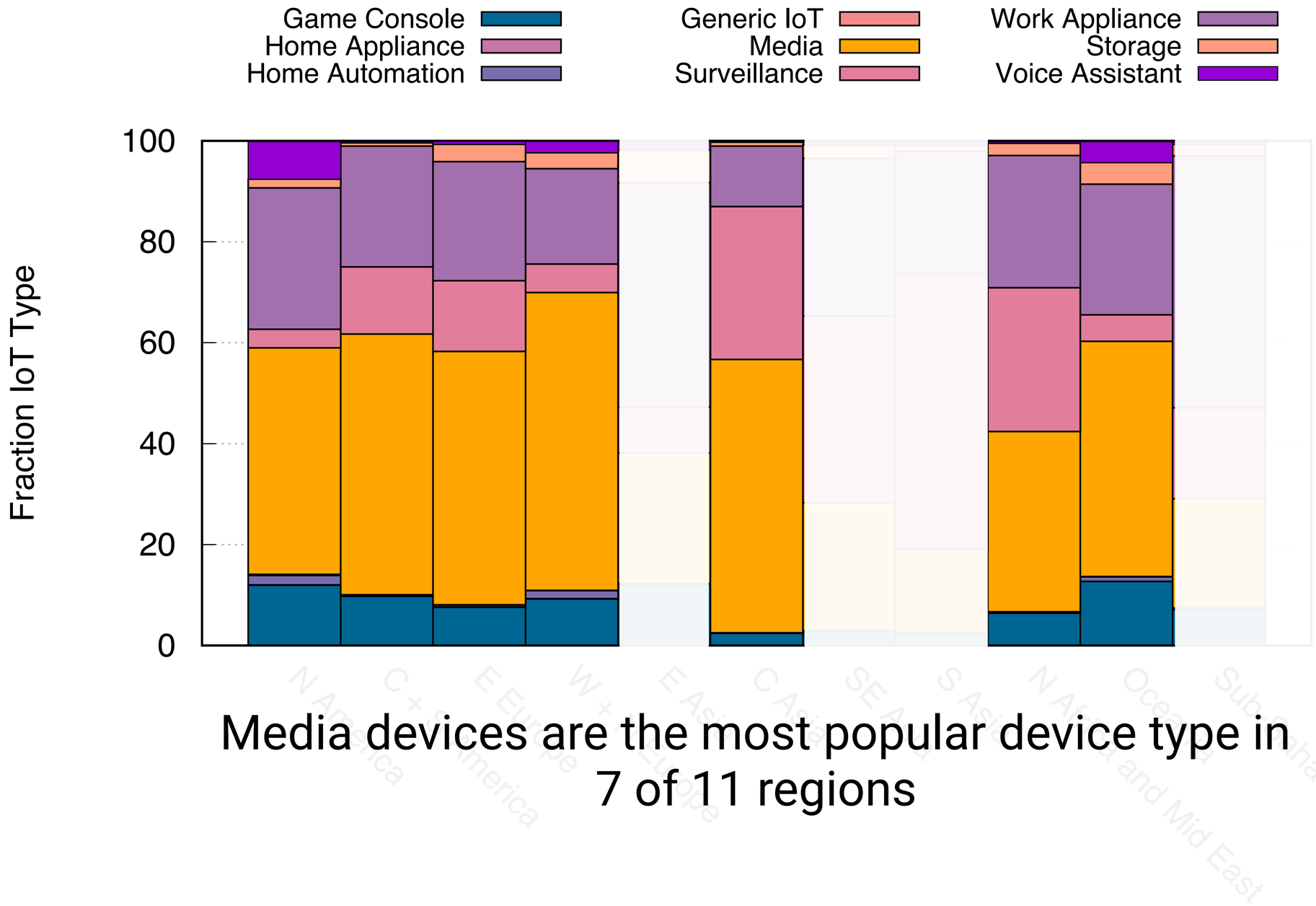
A Typical North American Home

Device Type	% of North American Homes
Media	**43%**
Work Appliance (e.g., printer)	**33%**
Gaming Console	**16%**
Voice Assistant	10%
Surveillance	4%
Storage (NAS)	3%
Home Automation (e.g., Nest)	2%
Wearable (e.g., watch)	0.2%
Other IoT	0.4%

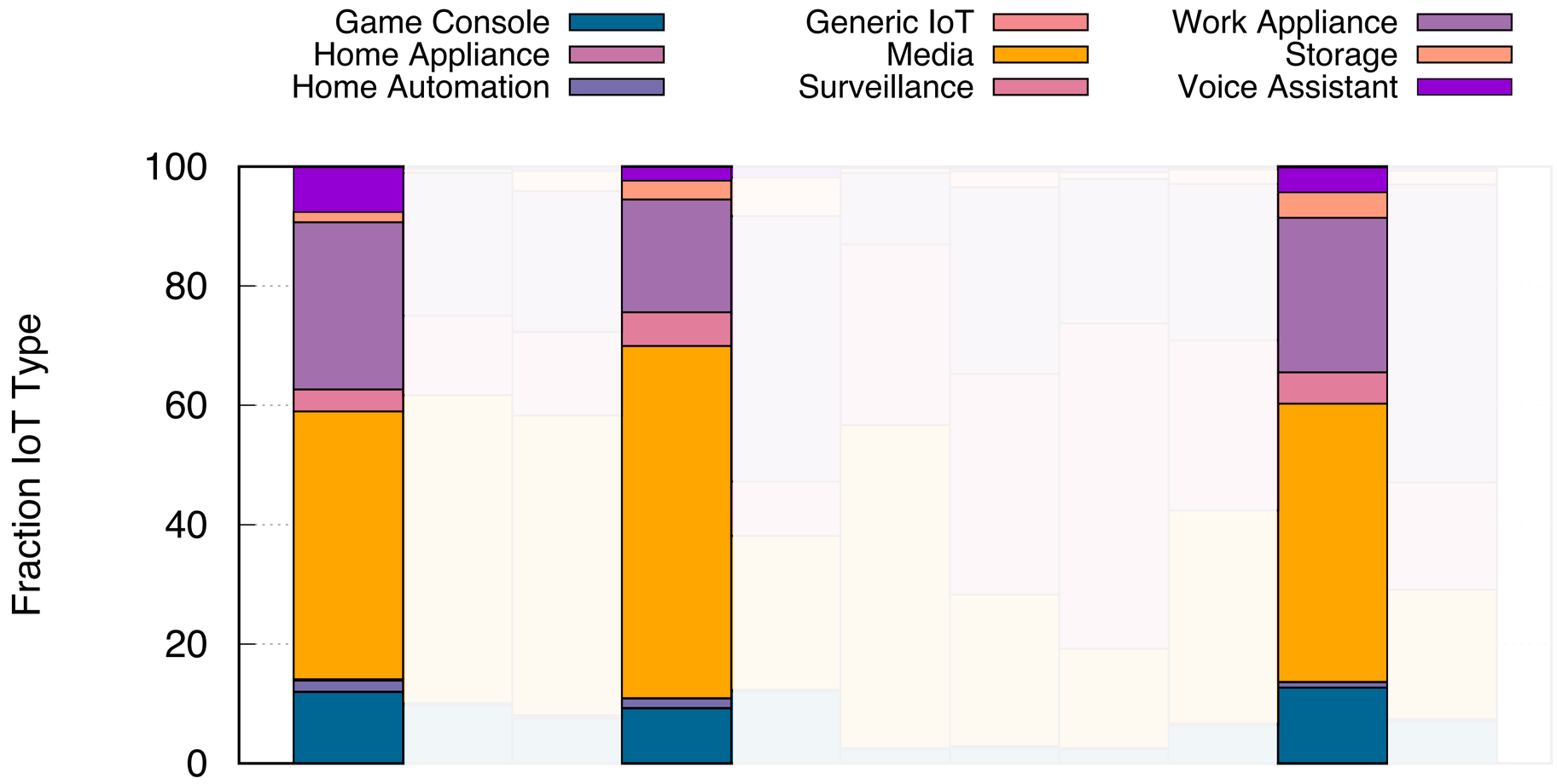
A Typical North American Home

Device Type	% of North American Homes
Media	43%
Work Appliance (e.g., printer)	33%
Gaming Console	16%
Voice Assistant	**10%**
Surveillance	4%
Storage (NAS)	3%
Home Automation (e.g., Nest)	**2%**
Wearable (e.g., watch)	0.2%
Other IoT	0.4%

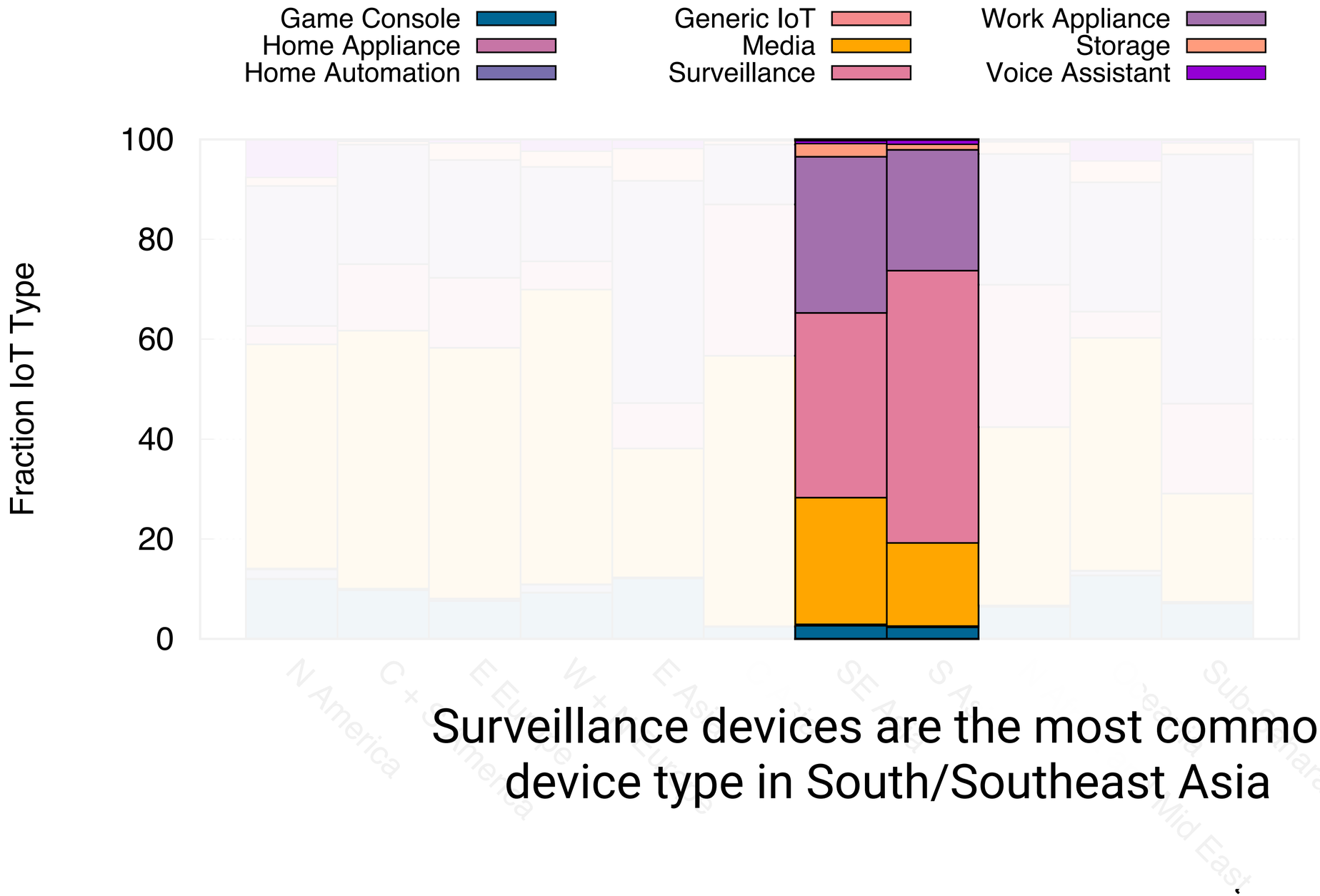

Game Console
Home Appliance
Home Automation
Generic IoT
Media
Surveillance
Work Appliance
Storage
Voice Assistant
Fraction IoT Type
100
80
60
40
20
0
N America
C + S America
E Europe
W + N Europe
E Asia
C Asia
SE Asia
S Asia
N Africa and Mid East
Oceania
Sub-Saharan Africa



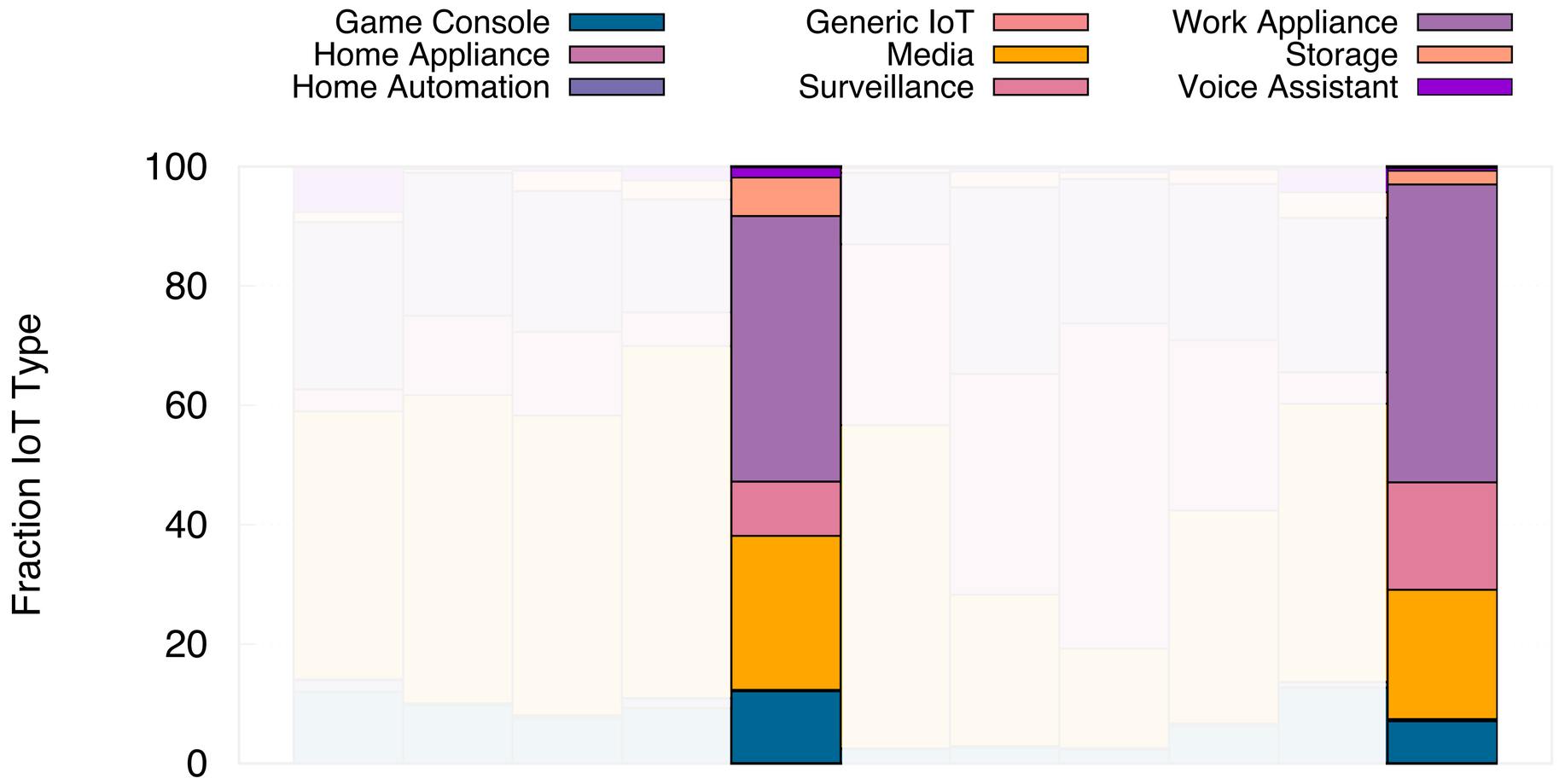
Media devices are the most popular device type in 7 of 11 regions



Home automation and voice assistants are only prevalent (>1% of homes) in North America, Western Europe, Oceania



Surveillance devices are the most common device type in South/Southeast Asia

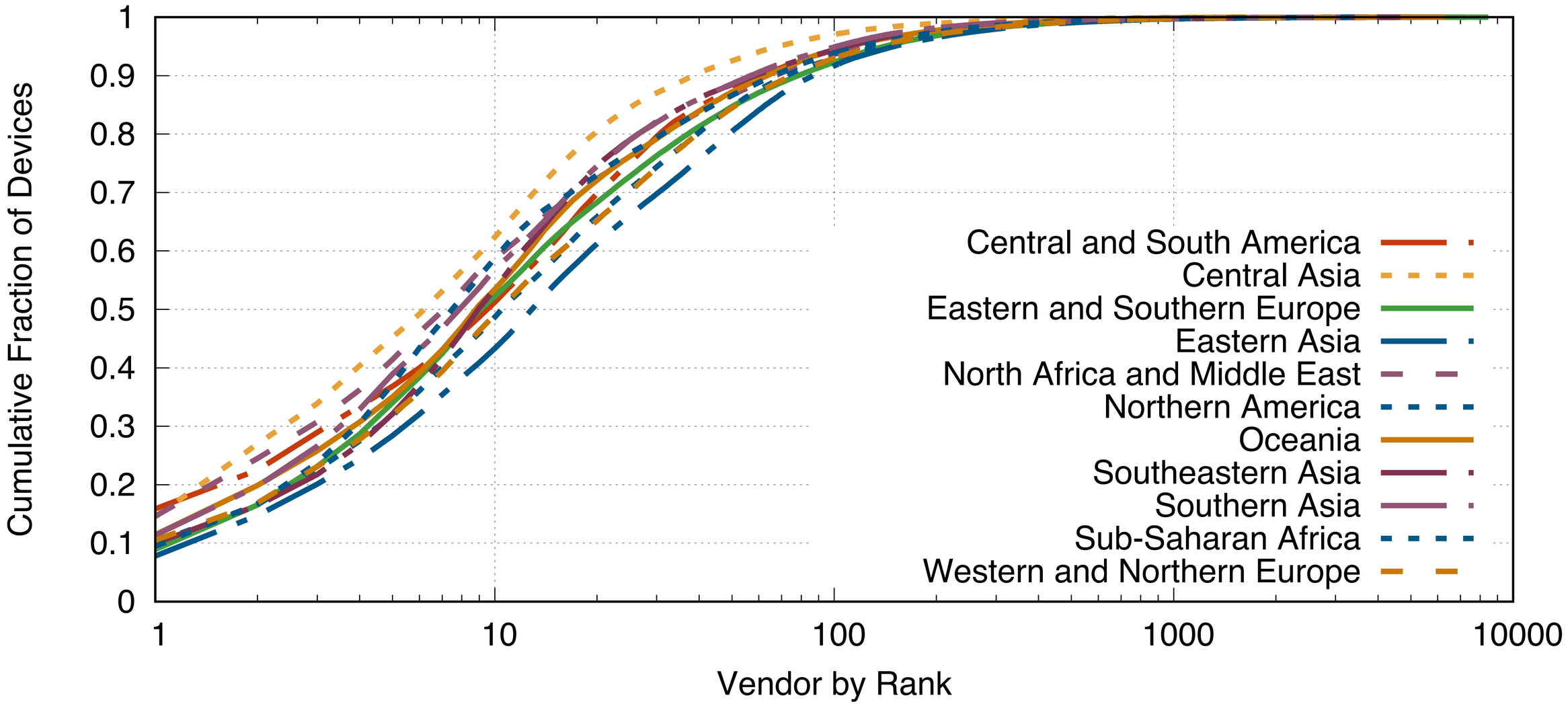


Work appliances are the most common device type in East Asia/Sub-Saharan Africa

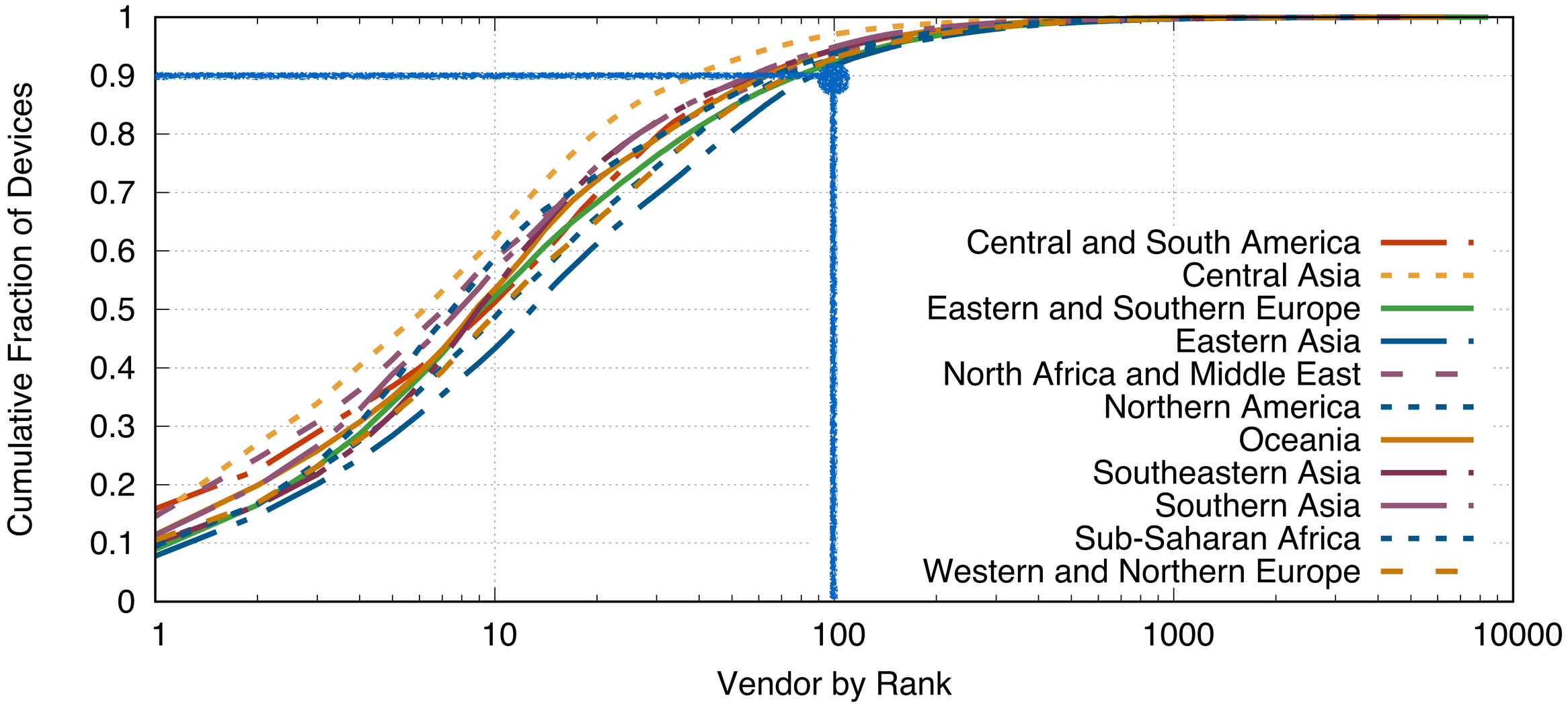
Each region has unique device type "preferences"

Who is making these devices?

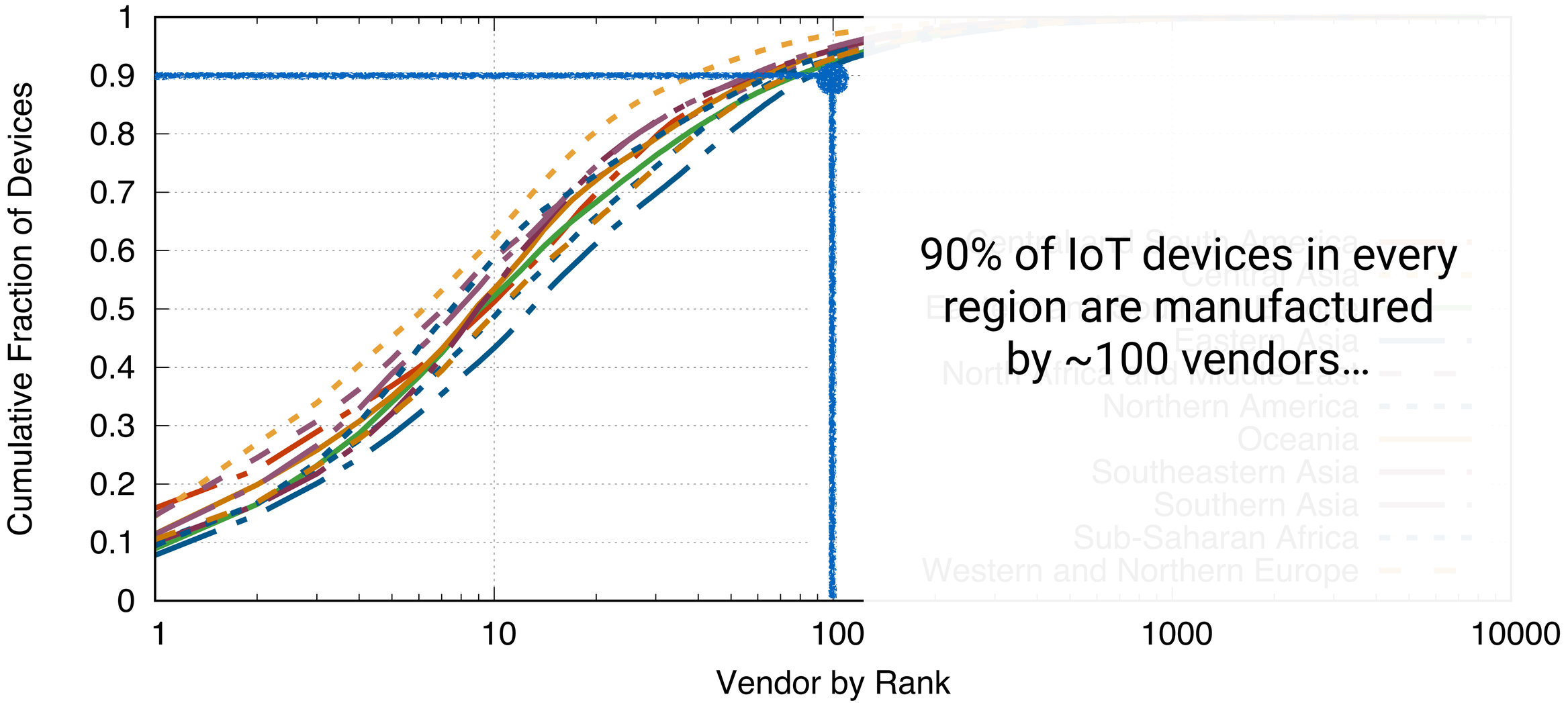
IoT Vendors by Region



IoT Vendors by Region

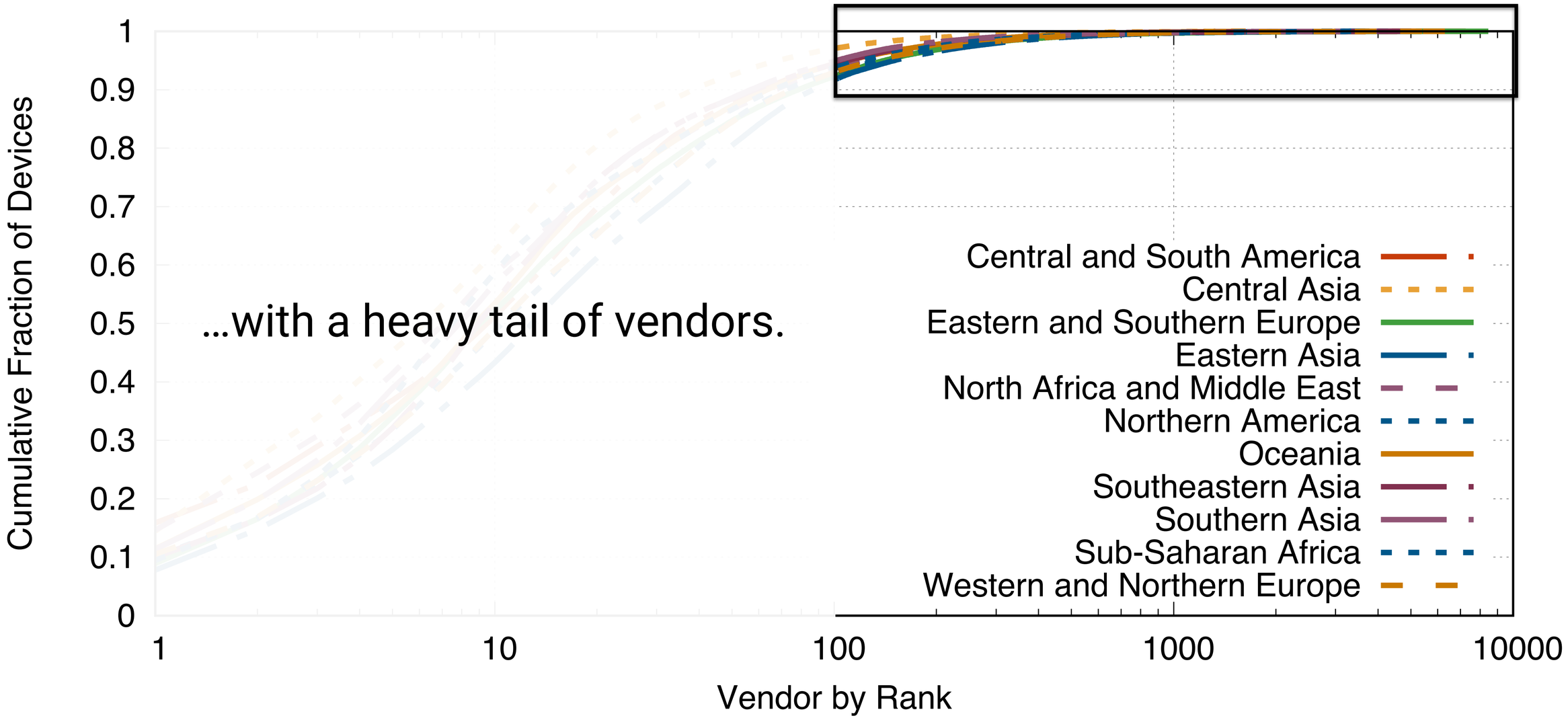


IoT Vendors by Region

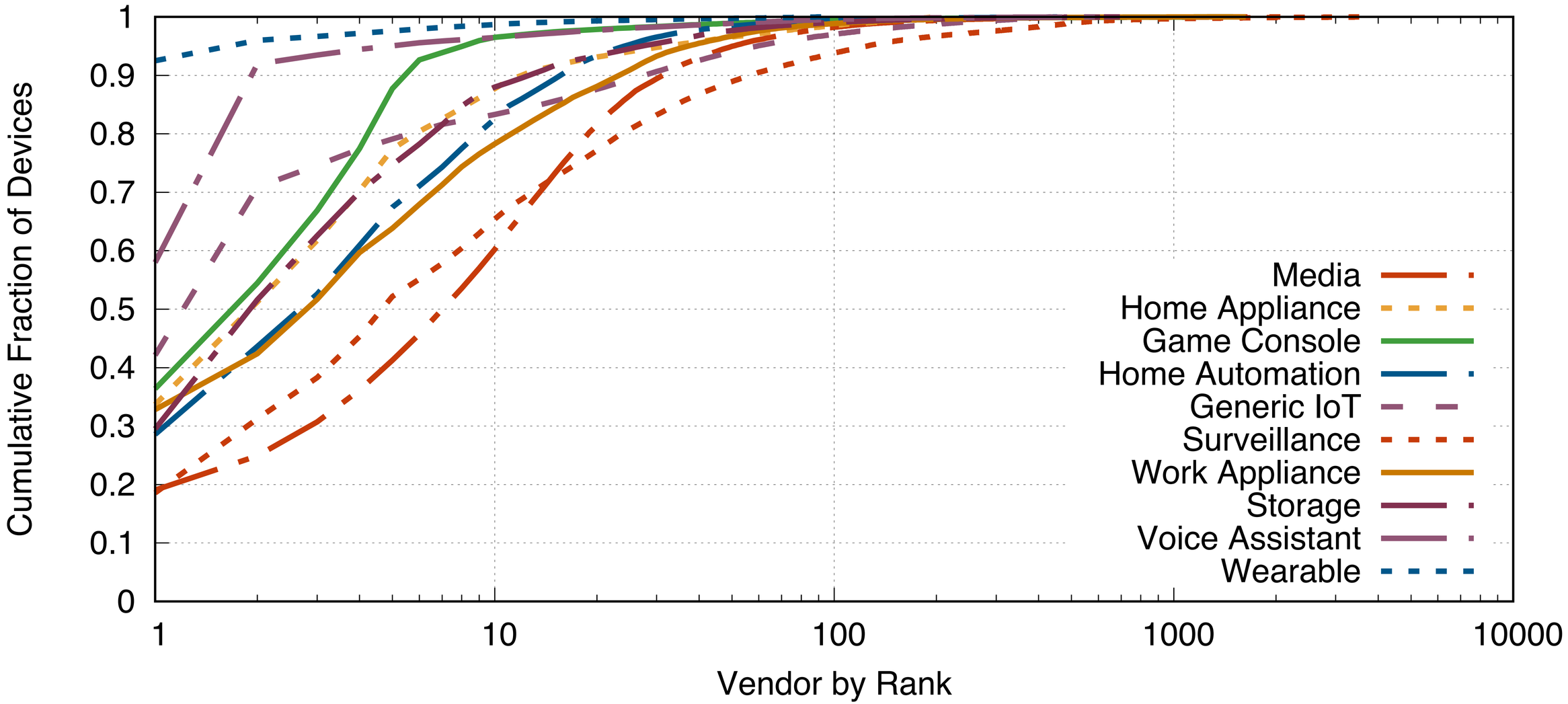


90% of IoT devices in every region are manufactured by ~100 vendors…

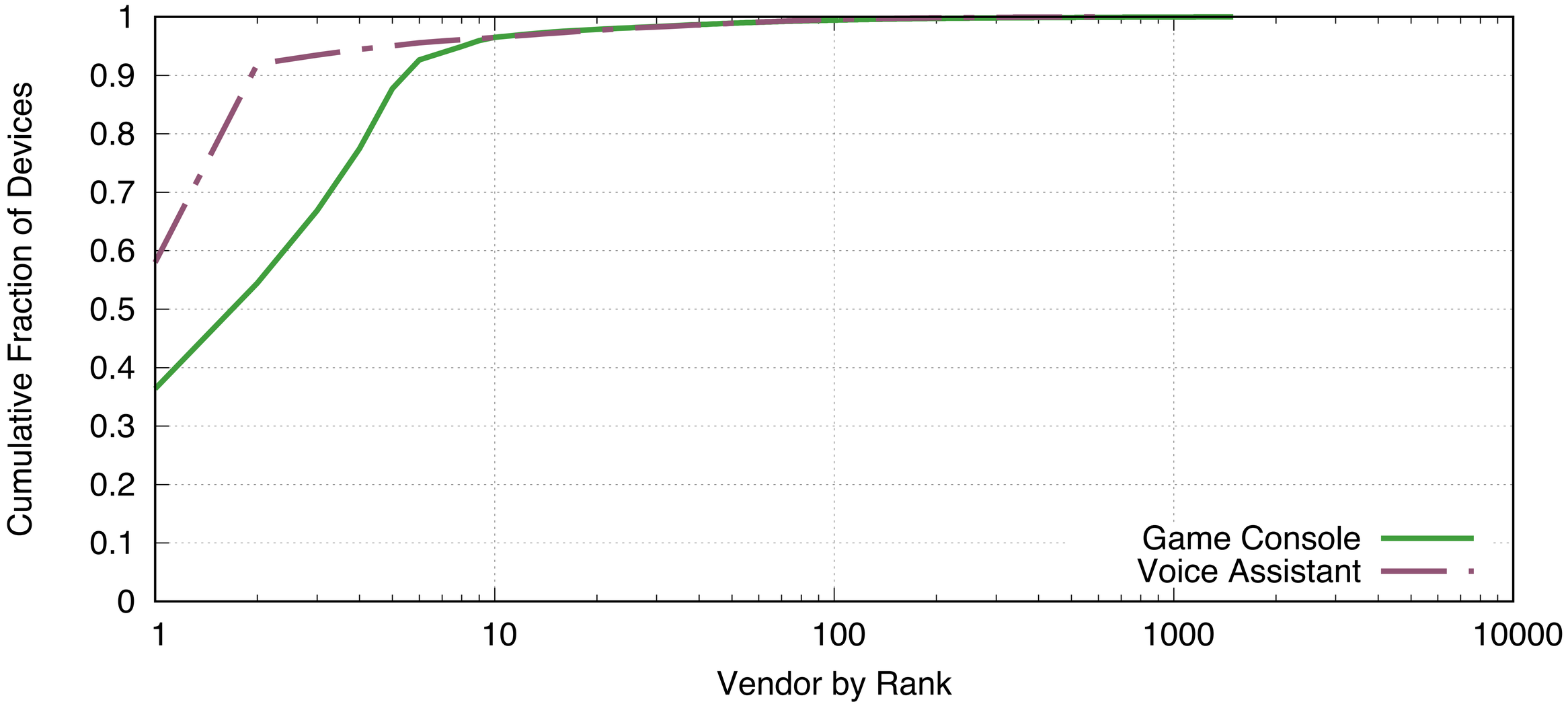
IoT Vendors by Region



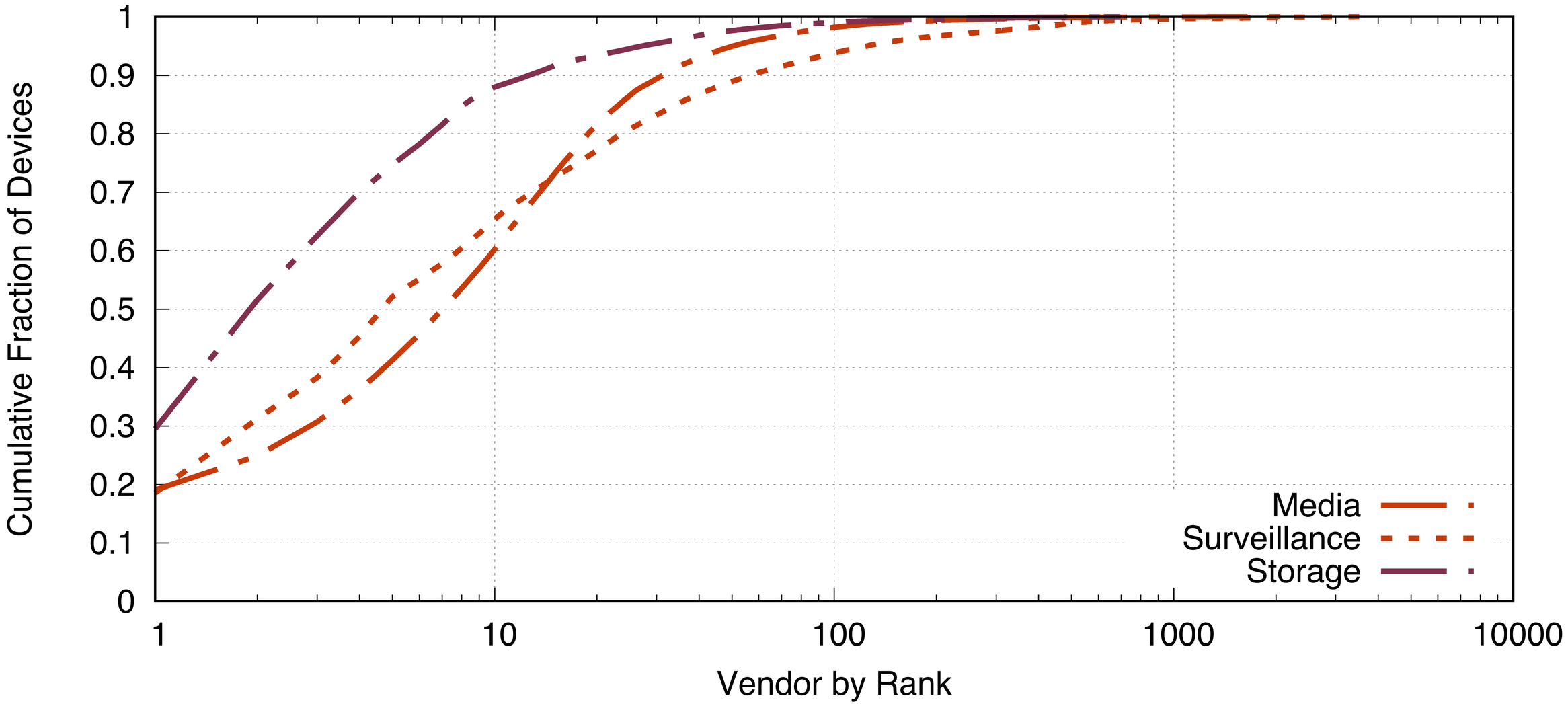
IoT Vendors by Device Type



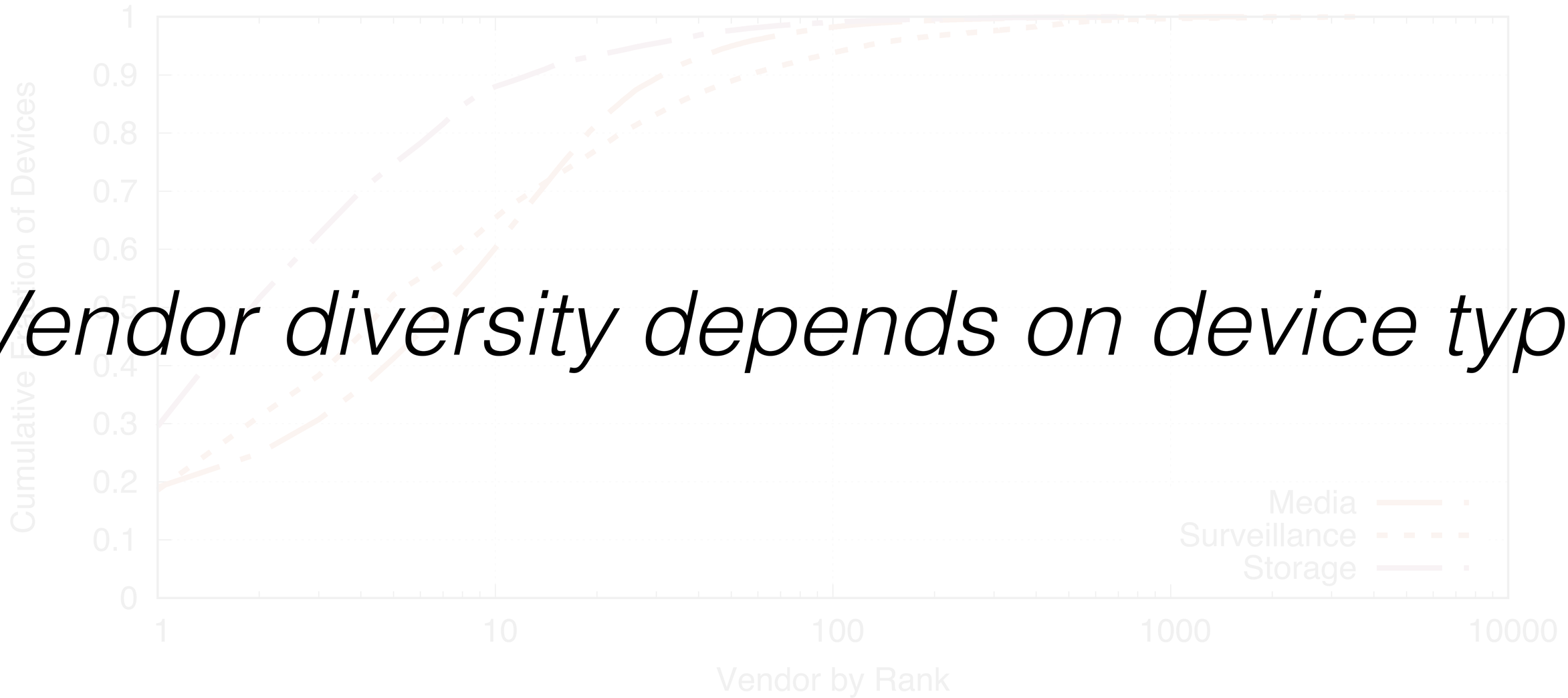
IoT Vendors by Device Type



IoT Vendors by Device Type



IoT Vendors by Device Type



Vendor diversity depends on device type

What does that mean for IoT security?

Weak Credentials

- “Security” is hard to measure in such a heterogeneous ecosystem

Weak Credentials

- “Security” is hard to measure in such a heterogeneous ecosystem
- We check weak credentials as a *proxy* for security

Weak Credentials

- “Security” is hard to measure in such a heterogeneous ecosystem
- We check weak credentials as a *proxy* for security
- **7.8%** devices support FTP, **7.1%** devices support Telnet

Weak Credentials

- “Security” is hard to measure in such a heterogeneous ecosystem
- We check weak credentials as a *proxy* for security
- **7.8%** devices support FTP, **7.1%** devices support Telnet
  - **17.4%** exhibit **weak FTP credentials**
  - **2.1%** exhibit **weak Telnet credentials**

Case Study: Weak Telnet Credentials

Device Type	% Support Telnet	% Weak Telnet
Surveillance	14.6%	10.7%
Router	14.6%	1.9%
Home Appliance	3.2%	1.6%
Media	1.4%	0.9%

Case Study: Weak Telnet Credentials

Device Type	% Support Telnet	% Weak Telnet
Surveillance	**14.6%**	**10.7%**
Router	**14.6%**	**1.9%**
Home Appliance	3.2%	1.6%
Media	1.4%	0.9%

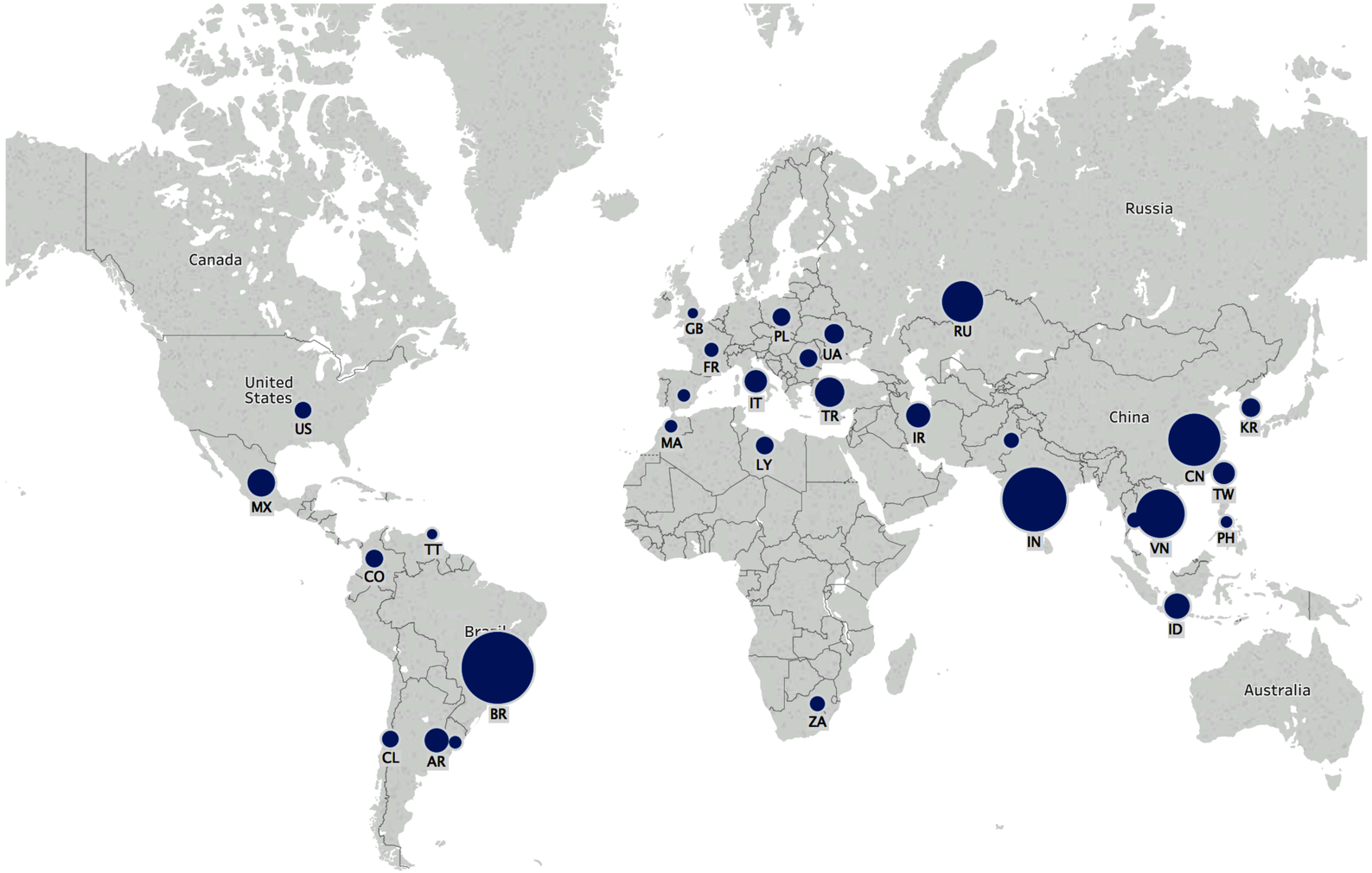
Case Study: Weak Telnet Credentials

Region	% IoT Weak Telnet	% Surveillance
North America	0.5%	3.7%
South America	4.9%	13.3%
Eastern Europe	3.0%	14.0%
Western Europe	1.0%	5.6%
East Asia	0.4%	9.1%
Central Asia	4.9%	30.3%
SE Asia	3.6%	37.0%
South Asia	2.9%	54.5%
Oceania	0.7%	4.3%
N. Africa + Middle East	4.8%	28.5%
Sub-Saharan Africa	1.1%	18%

Case Study: Weak Telnet Credentials

Region	% IoT Weak Telnet	% Surveillance
North America	0.5%	3.7%
South America	**4.9%**	**13.3%**
Eastern Europe	**3.0%**	**14.0%**
Western Europe	1.0%	5.6%
East Asia	0.4%	9.1%
Central Asia	**4.9%**	**30.3%**
SE Asia	**3.6%**	**37.0%**
South Asia	**2.9%**	**54.5%**
Oceania	0.7%	4.3%
N. Africa + Middle East	**4.8%**	**28.5%**
Sub-Saharan Africa	**1.1%**	**18%**

Mirai Infections



Security challenges *vary* per region depending on device preferences

Takeaways

- Home IoT ecosystem is diverse and fragmented

Takeaways

- Home IoT ecosystem is diverse and fragmented
  - Regional differences in # of devices, device types, and device vendors

Takeaways

- Home IoT ecosystem is diverse and fragmented
  - Regional differences in # of devices, device types, and device vendors
- Quantifying IoT security at scale remains an outstanding challenge

Takeaways

- Home IoT ecosystem is diverse and fragmented
  - Regional differences in # of devices, device types, and device vendors
- Quantifying IoT security at scale remains an outstanding challenge
- IoT has *been* here… for years

Takeaways

- Home IoT ecosystem is diverse and fragmented
  - Regional differences in # of devices, device types, and device vendors
- Quantifying IoT security at scale remains an outstanding challenge
- IoT has *been* here… for years

Questions?
dkumar11@illinois.edu
@_kumarde