MCCA
GLOBAL TEC
FORUM
MCCA Celebrating 20 Years

# JUNE
# 19 AND 20

AT THE
INTERCONTINENTAL
SAN FRANCISCO

**Smita Rajmohan**
Counsel,
Technology Transactions

**Maulik Shah**
Counsel,
Adobe Systems Incorporated

**Shannon Yavorsky**
Partner,
Venable LLP

## Internet of Things (IoT): Legal and Privacy Issues

Join MCCA and several leading IoT experts at our annual Global TEC Forum (G-TEC) on Tuesday, June 20, 2017 for this tech-savvy panel.

For more information and to register please visit: **www.mcca.com/gtec**

# The Internet of: Unsecure Things

- Connected Toys
  - Recent case involving a doll
- Connected Consumer Goods
  - Baby monitor
- Risks: (i) hacking the device itself; and (ii) a breach of the data generated by the device

# The Internet of: Hard-to-Secure Things

## Samsung S8 Iris Scanner:

http://mirror.netcologne.de/CCC/contributors/berlin/biometrie/h264-sd/biometrie-11-eng-Hacking_the_Samsung_Galaxy_S8_Irisscanner_sd.mp4

## iPhone Fingerprint Scanner

https://youtu.be/fZJI_BrMZXU

## HSBC Voice Recognizer

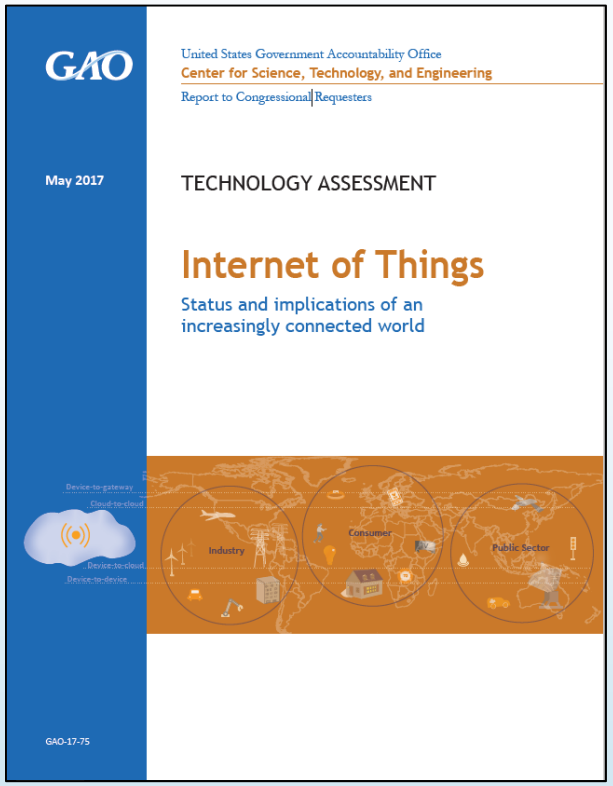
http://www.bbc.com/news/technology-39965545

## Machine Learning Based Voice Synthesizers

- LyreBird: https://www.theverge.com/2017/4/24/15406882/ai-voice-synthesis-copy-human-speech-lyrebird
- Adobe Voco: https://www.youtube.com/watch?v=I3l4XLZ59iw
- Google Deepmind: https://www.theverge.com/2016/9/9/12860866/google-deepmind-wavenet-ai-text-to-speech-synthesis

# The Internet of: Big-Brother-Is-Watching Things

**"Privacy.** Smart devices that monitor public spaces may collect information about individuals without their knowledge or consent. For example, fitness trackers link the data they collect to online user accounts, which generally include personally identifiable information, such as names, email addresses, and dates of birth. Such information could be used in ways that the consumer did not anticipate. For example, that data could be sold to companies to target consumers with advertising or to determine insurance rates."



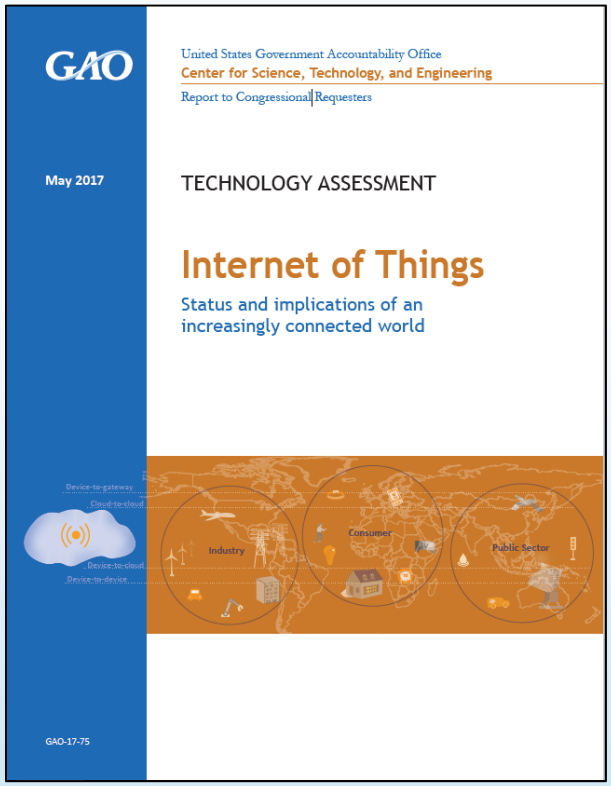

**Burger King Prank:**

- https://youtu.be/U_O54le4__I

# The Internet of: Cyber-weapon Things

**Information security.** The IoT brings the risks inherent in potentially unsecured information technology systems into homes, factories, and communities. IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. For example, in 2016, hundreds of thousands of weakly-secured IoT devices were accessed and hacked, disrupting traffic on the Internet.

**Safety.** Researchers have demonstrated that IoT devices such as connected automobiles and medical devices can be hacked, potentially endangering the health and safety of their owners. For example, in 2015, hackers gained remote access to a car through its connected entertainment system and were able to cut the brakes and disable the transmission.



# Contracts:

## IoT Provider Side

**DATA BREACH:** You agree to immediately notify [IoT Provider] of any unauthorized use, or suspected unauthorized use, of your account or any other breach of security. [IoT Provider] is not liable for any loss or damage arising from your failure to comply with the above requirements. [IoT Provider] cannot guarantee that unauthorized third parties will never be able to defeat our security measures or use your personal information for improper purposes. You acknowledge that you provide your personal information at your own risk.

**TERMINATION:** At any time, [IoT Provider] may (i) suspend or terminate your rights to access or use the Services

**UPDATES:** [IoT Provider] may from time to time develop patches, bug fixes, updates, upgrades and other modifications to improve the performance of the Services and/or the Product Software. These may be automatically installed without providing any additional notice or receiving any additional consent. You consent to this automatic update.

# Contracts:

## IoT Provider Side

**APPLICABLE LAW:** You agree that you are responsible for ensuring that you comply with any applicable laws when you use the Products and Services.

**INDEMNITY:** You agree to defend, indemnify and hold [IoT Provider] and its licensors and suppliers harmless from any damages, liabilities, claims or demands (including costs and attorneys' fees) made by any third party due to or arising out of (i) your use and each Authorized User's use of the Products or Services, (ii) your or your Authorized Users' violation of these Terms, (iii) any User Submissions or Feedback you provide; or (iv) your or your Authorized Users' violation of any law or the rights of any third party.

**WARRANTY:** THE SERVICES ARE PROVIDED FOR YOUR CONVENIENCE, "AS IS" AND "AS AVAILABLE" AND [IoT Provider] AND OUR LICENSORS AND SUPPLIERS EXPRESSLY DISCLAIM ANY WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, AND NON-INFRINGEMENT.

# Deal Documents:
## Purchase Agreement Reps

*The Company has implemented industry standard systems and procedures related to information security and intended to **prevent unauthorized access** to the Business Systems **and** the introduction of **any Malicious Code** to the Business Systems, including by **implementing systems and procedures** (i) that manage mobile devices, including those provided to employees or contractors by the Company and those provided by such individuals themselves (and the Company does not permit such individuals to use devices in connection with the Business that are not monitored by the Company), (ii) that **provide continuous monitoring and alerting of any deficiencies, problems or issues** with the Business Systems, and (iii) that **monitor network traffic** for threats and scan and assess vulnerabilities in the Business Systems.*

# Deal Documents:
## Purchase Agreement Reps

*"The Company has implemented **industry standard systems** and procedures and a notification of any problems identified by such systems and procedures is provided automatically and immediately to the Company's Information Officer."*

# Deal Documents:
## Purchase Agreement Reps

*The Company has implemented commercially-reasonable **training programs and formal policies** to ensure training of all of the Company's employees and contractors with respect to information security and cybersecurity issues, and such training programs and formal policies are **updated no less often than annually**."*

# Deal Documents:
## Purchase Agreement Reps

- *The Company has implemented **multi-factor authentication for external access** to the Business Systems."*

- *The Company **carries cybersecurity insurance** in the amounts and **with the limitations** described on Schedule [X]"*

# EU General Data Protection Regulation - the "GDPR"

- Comes fully into effect May 25, 2018
  - Territorial scope
  - Fines (up to 4% of annual worldwide turnover or 20 million euros, whichever is higher)
  - Personal data – expanded definition
  - Consent
  - Children
  - Data subjects' rights
  - Accountability
  - Cross border data transfer
  - Data security

# General Data Protection Regulation

- Privacy by Design – Data controllers may need to conduct data protection impact assessments in connection with IoT devices.
- Consent – the GDPR tightens existing requirements in relation to consent. How will IoT devices obtain consent?
- Security – both data controllers *and data processors* need to meet enhanced obligations with respect to data security.
- Data Breach – under the new law data controllers are required to report personal data breaches no later than 72 hours after becoming aware of the breach.