TRUSTONIC

Beyond mobile

Richard Hayton, CTO

October 2017

CONFIDENTIAL

Two views of security

To keep you out

To let you in

New, Better, less Risky
Experiences

IOT is

BIG

Really Big.

You just won't believe how vastly, hugely, Mind-bogglingly big it is.

I mean, you may think it is a long way down the road to the chemist, but that's *peanuts* to IOT!

But what comes next….

Mobile devices are the culmination of what has become known as the third industrial revolution
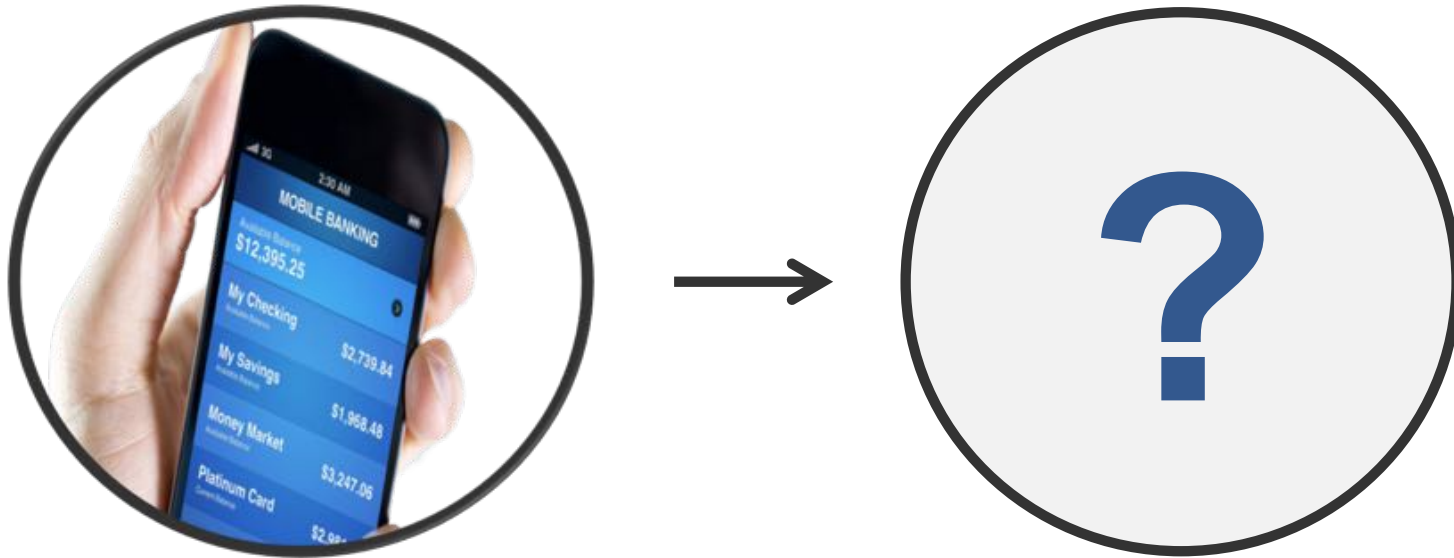
TRUSTONIC

But what comes next....

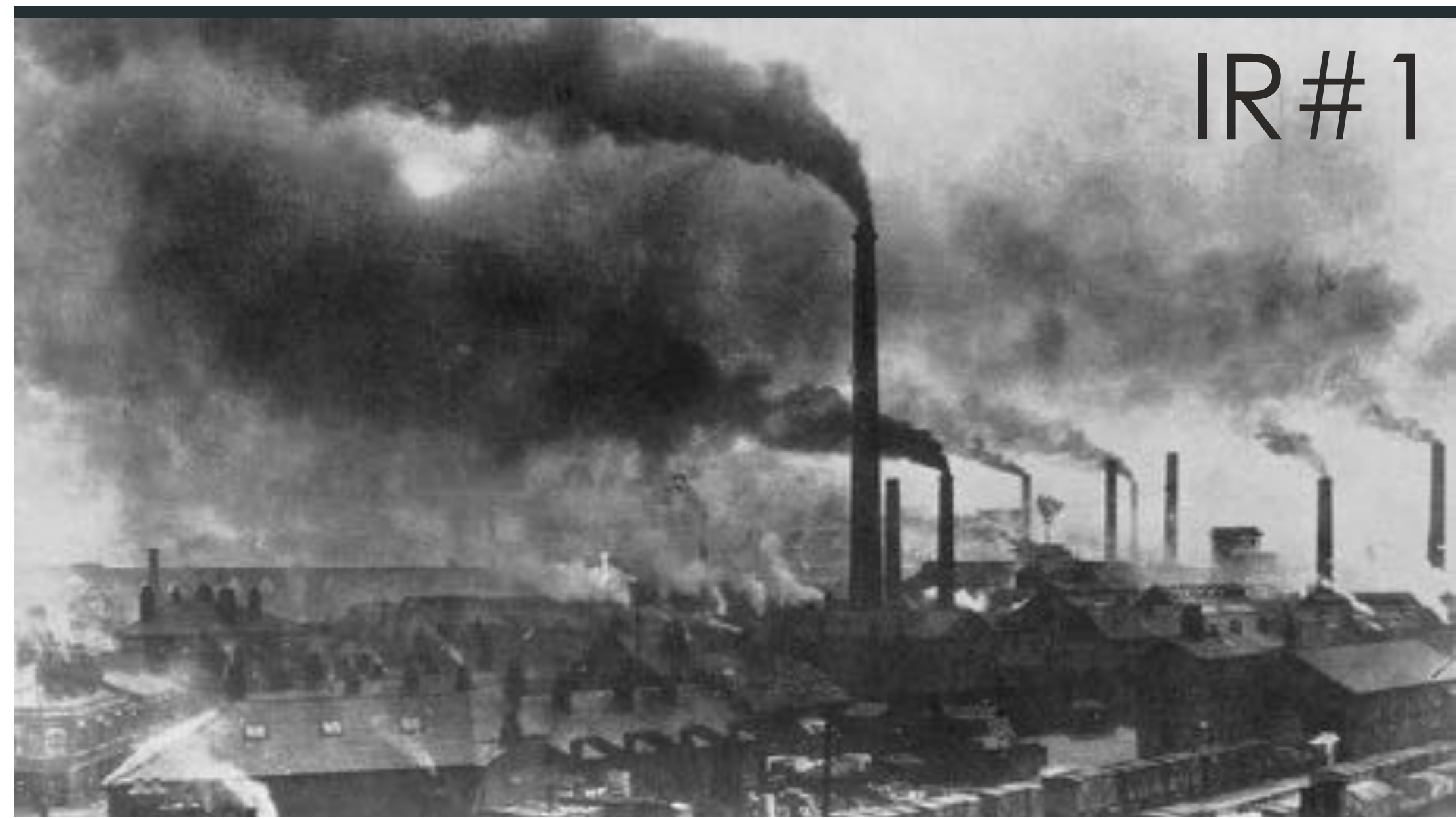Mobile devices are the culmination of what has become known as the third industrial revolution

How do we apply what we have learned to the fourth industrial Revolution, IoT

TRUSTONIC

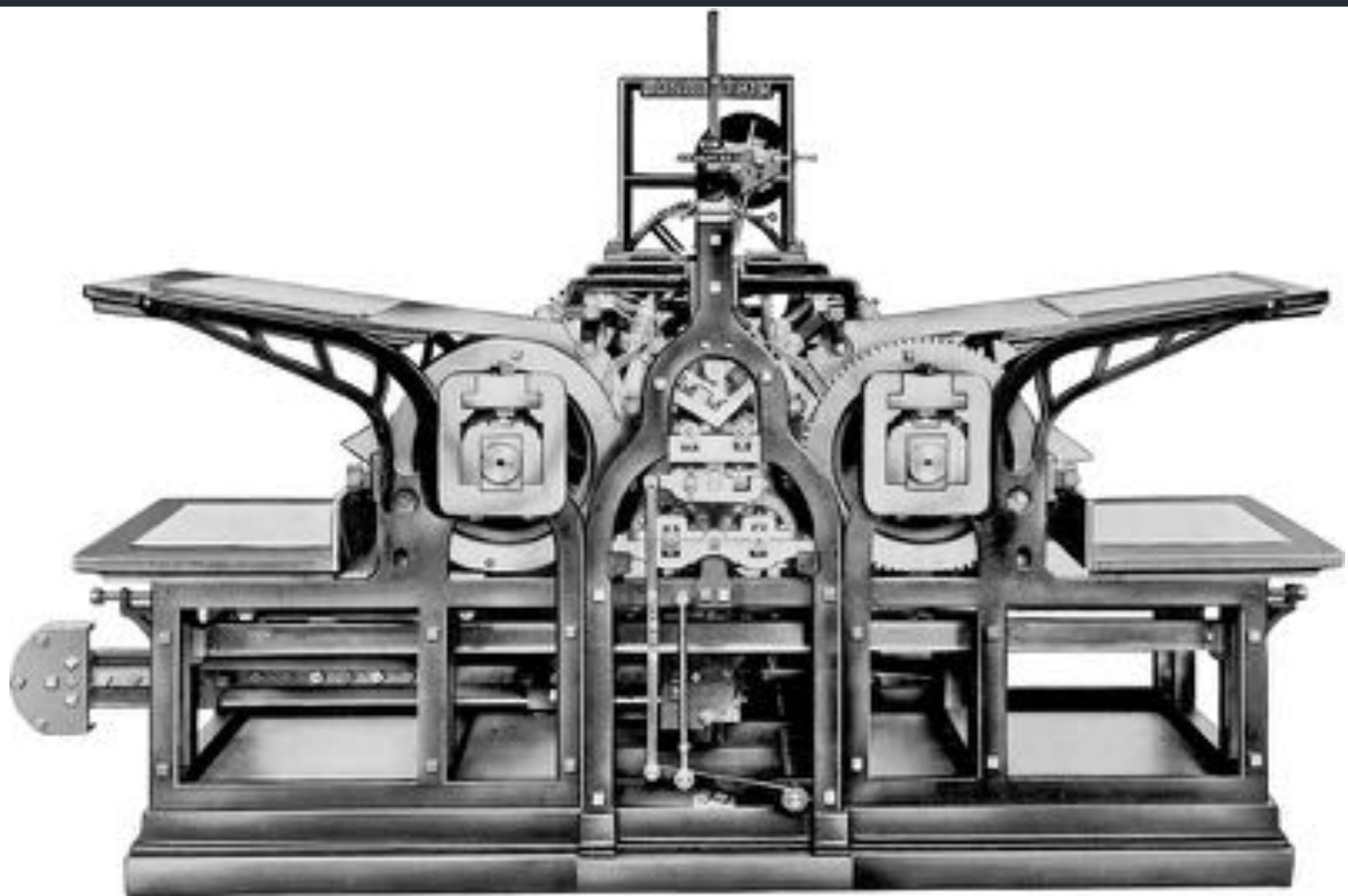# But what comes next....

In this talk we will look at what we can learn from the from the first three industrial revolutions and apply what we learn to the fourth.

TRUSTONIC

IR#1

This lead to a new industry of popular literature

With IoT, we are seeing a similar rush by companies to embrace the new technology

Does security on the end device really matter?

Kinibi & Kinibi-M for IoT
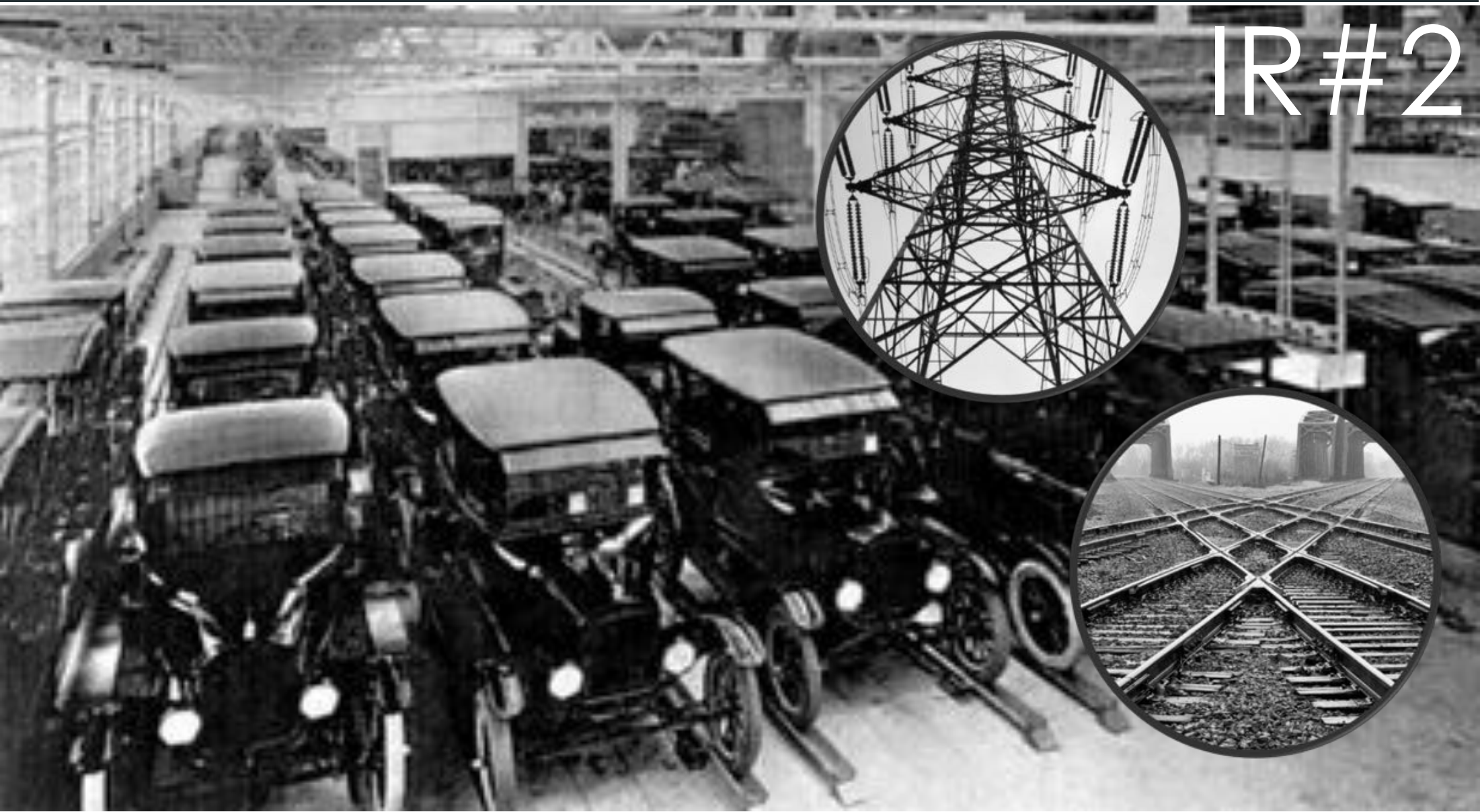
Full TEE-OS for A Class Processors

Global Platform APIs

Flexible cryptography

Secure code separation…

Modular software for M Class Processors

Global Platform *inspired* APIs

Flexible cryptography

Secure code separation…

TRUSTONIC
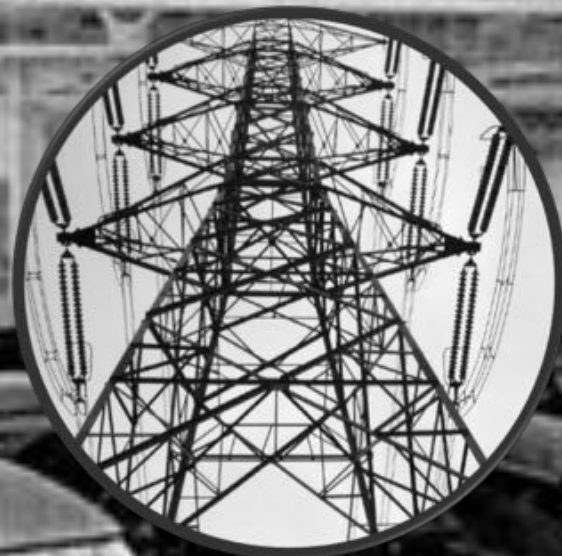
Enabling device trust

Devices must be…

Legitimate – to avoid fraudulent clients and fake components and devices

Identifiable – linked to an account or purpose during operational lifetime.

Protected – Combating new threats and exploits require secure in-field automatic update

Trustonic introduces Digital Holograms

© ABC Corp.
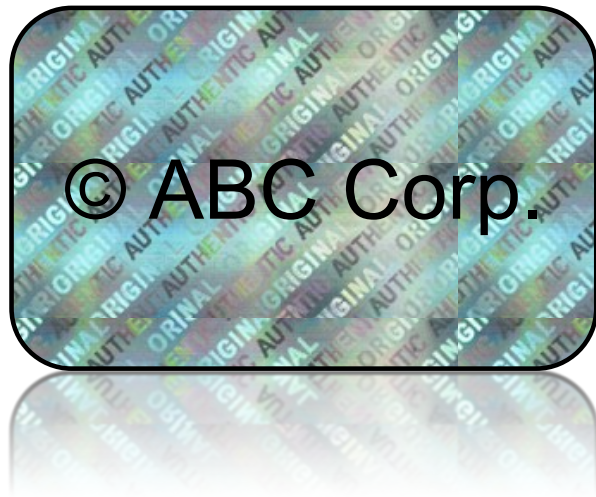
These are a new technology to allow anyone in the device manufacturing chain to securely and *irreversibly* attest to a stage of manufacture

Flexible "branding" to enable trust:

- Module Maker, QA, Model Identification

- Assignment to company/user

- Maintenance

- End of Life

- Etc.
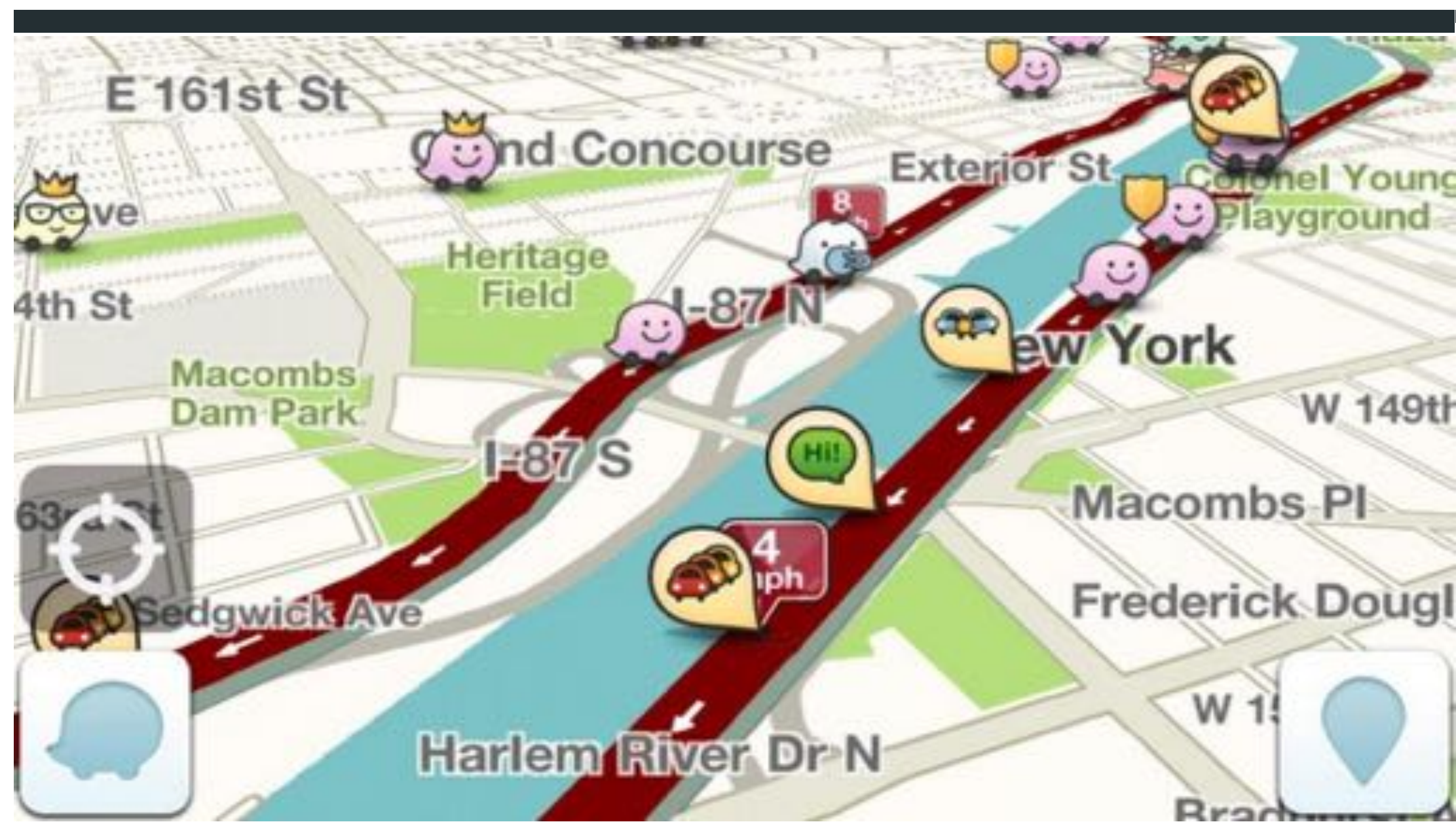
TRUSTONIC

IR#3

WIKIPEDIA
The Free Encyclopedia

English
5 501 000+ articles

Español
1 361 000+ artículos

日本語
1 081 000+ 記事

Deutsch
2 115 000+ Artikel

Русский
1 430 000+ статей

Français
1 923 000+ articles

Italiano
1 393 000+ voci

中文
971 000+ 條目

Português
981 000+ artigos

Polski
1 247 000+ haseł

EN

False GPS signals transmitted by attacker

IEEE Spectrum

Health
Trial
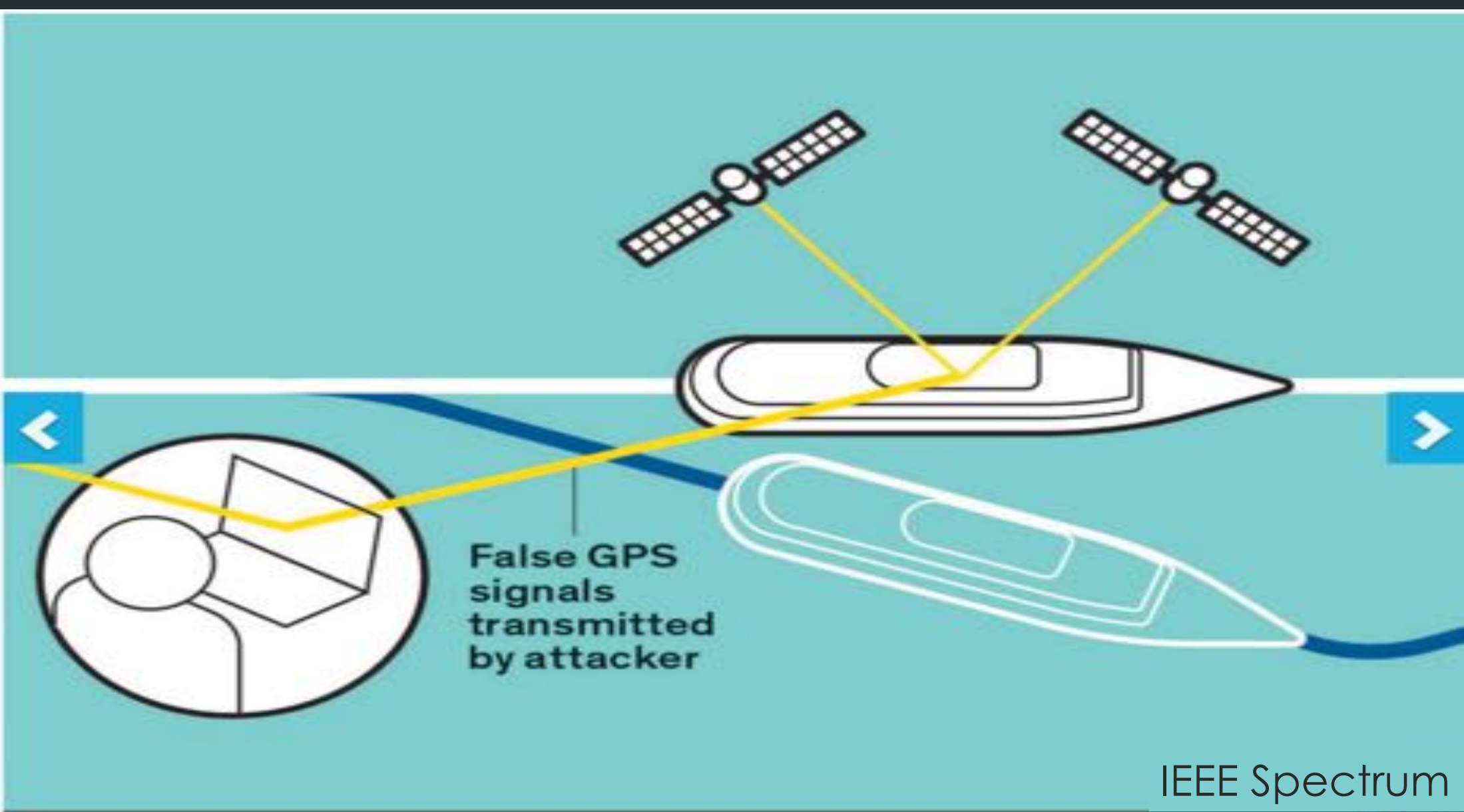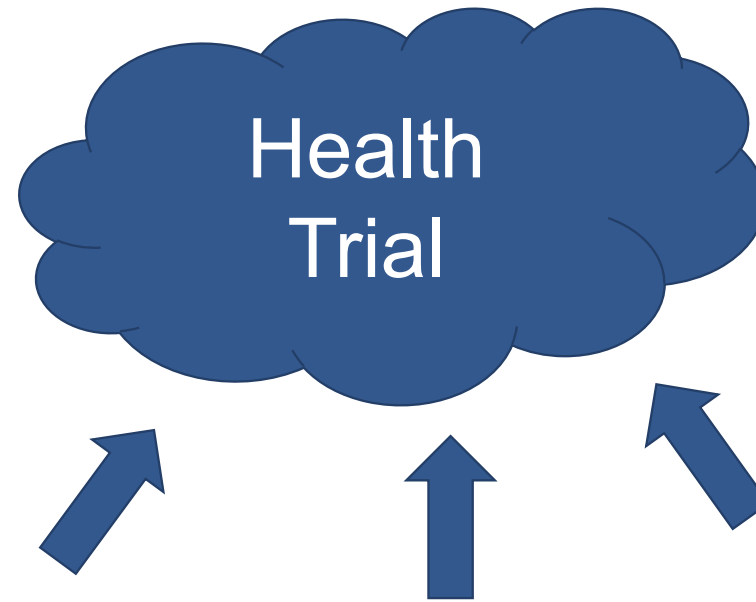
TRUSTONIC

Establishing a framework for Trust

"Trust me I'm a Robot" & "A Matter of Policy"

https://www.trustonic.com/news/category/blog/

TRUST☉NIC

CONFIDENTIAL

IR#4

What will be unique about the
IoT Revolution?

TRUSTONIC

New class of actor…

Not necessarily full blown robots…

But devices doing things that used
to be preserve of humans

Seriously?

iPhone Software Update

3. Transfer. You may not rent, lease, lend, sell, redistribute, or sublicense the iOS Software. You may, however (a)

Oh you know what? This is page 46, nobody's still reading this. I bet only about five people clicked to read the T&Cs in the first place – we might as well just say anything we like.

Tony on floor 5 of Apple HQ smells of sardines.

When someone sends a funny email around the offices we have to reply with iLaughed. It's in our job description.

Remember that legal battle over Apple & Apple studios? Want to know [...] fight The Beatles. We have the surviving ones come [...] aps. We're looking at ways to reanimate the dead ones.

[...] apple products. Apples, apple juice, apple flapjacks, [...]. We [...] ed if we're caught eating anything without apples [...] LLERG [...] APPLES AND I'M ALWAYS SO HUNGRY.

[...] aked the [...] landings. Did it in 2008, then brainwashed you all to [...] ve it happened in 1969, just because we could. If anyone finds out [...] ve leaked this information, I'll be killed. But no one will ever, ever read this.

(b) you do not retain any copies of the iOS Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the iOS Software reads and agrees to accept the terms and conditions of this License.

Decline   Agree

- *Really Smart Meter*

- *Control my electricity usage*

- *Buy (or sell) electricity on the open market*

Who might be behind a hack…

"End User"?

- Get free electricity.

"Terrorists"?

- Overload grid? Burn down house? …

"Criminals"

- Manipulate energy market

"Power Companies"

- Use more power – work for supplier not consumer…

"Insurance Companies"

- Spy on homeowners to determine risk

"Governments"

- Enforce policies / "lifestyles". Overreach…

TRUSTONIC

One penny on each transaction…

What we have learned…

Breadth of impact across industries

(e.g. Printing)

Unanticipated effects lead to new opportunities and challenges

Large change scale Leads to huge competition In new areas

(E.g. Consumerization)

Need to establish Trust in your brand

Decentralized control changes more than technology

(E.g. Wikipedia→ Social Media)

Flexibility is needed as the rules will change as the technology evolves

Non Human Actors change everything

(E.g. Smart Meter)

Significant new challenges to trust as 'armies' of devices are targeted by attackers

TRUSTONIC

Its all about Trust

Flexible Policies

Validation & Certification

Secure Software

Secure Manufacture

Thank you

Richard Hayton
CTO

TRUSTONIC