Do Now:

1. Say hello to your neighbor!
2. Think of an OS you use. Discuss what you use it for and how you trust it.

CS111 Lecture
OS Trust in Context

Benjamin Xie, Ph.D.

Embedded Ethics Fellow
benjixie@stanford.edu | benjixie.com

made with William Grant Ray III, Xiyu Zhang, Liana Keesing, Swayam Parida, Prof. Nick Troccoli, Prof. John Ousterhout

A mysterious bug

```
year = ORIGINYEAR; /* = 1980 */

while (days > 365) {
    if (IsLeapYear(year)) {
        if (days > 366) {
            days -= 366;
            year += 1;
        }
    }
    else {
        days -= 365;
        year += 1;
   }
}
```

The following code handles the clock driver for a device.

This code contains a bug that affects the device one day every four years.

Discuss with your neighbor why.

Edge cases, y’all

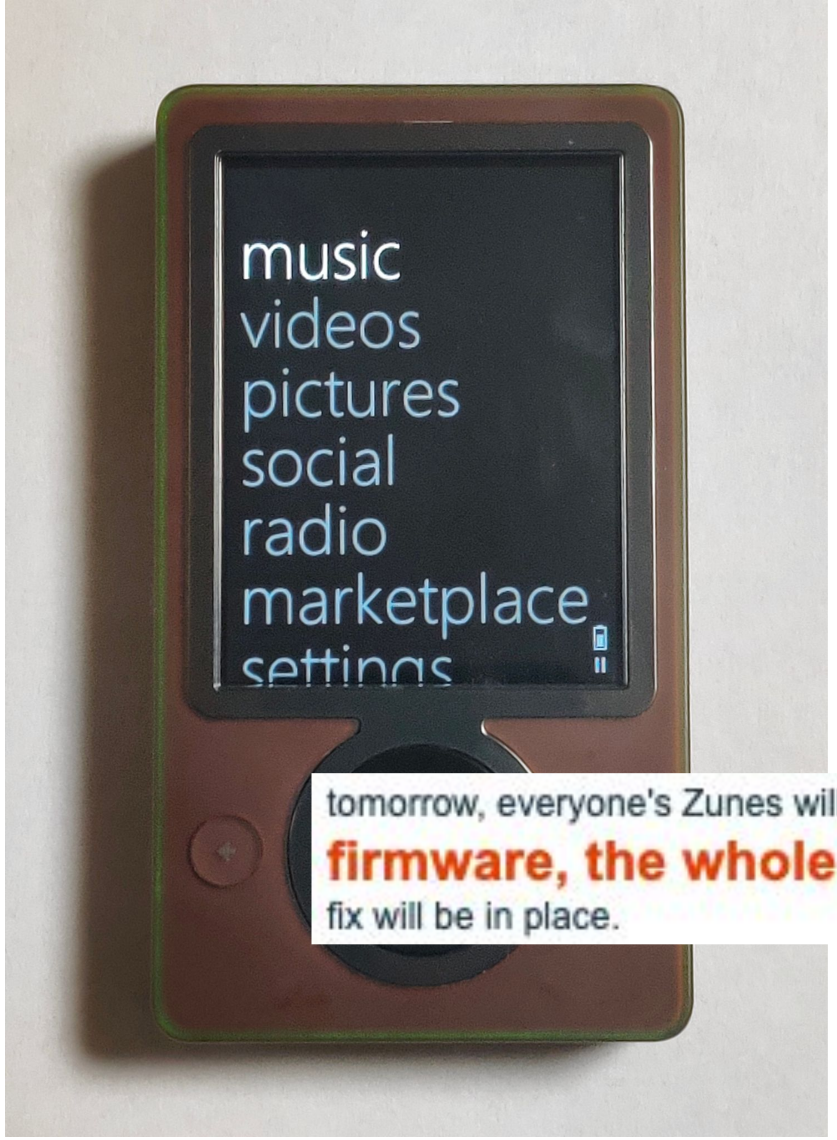
```
year = ORIGINYEAR; /* = 1980 */

while (days > 365) {
    if (IsLeapYear(year)) {
        if (days > 366) {
            days -= 366;
            year += 1;
        }
    }
    else {
        days -= 365;
        year += 1;
   }
}
```

No else condition

=> stuck in while loop on last day of leap year (until days > 366)

music
videos
pictures
social
radio
marketplace
settings

The day the Zune stood still



On 31 Dec 2008 (last day of leap year), Zune 30s froze.

Solution: let battery run out and bug will disappear next day 🤷

tomorrow, everyone's Zunes will operate normally again. However, **if Microsoft doesn't fix this part of the firmware, the whole thing will happen all over again in 4 more years.**. Hopefully by then a fix will be in place.

Microsoft discontinued Zunes less than 4 years later…

What is needed to build a trustworthy OS?

How does the deployment context matter?

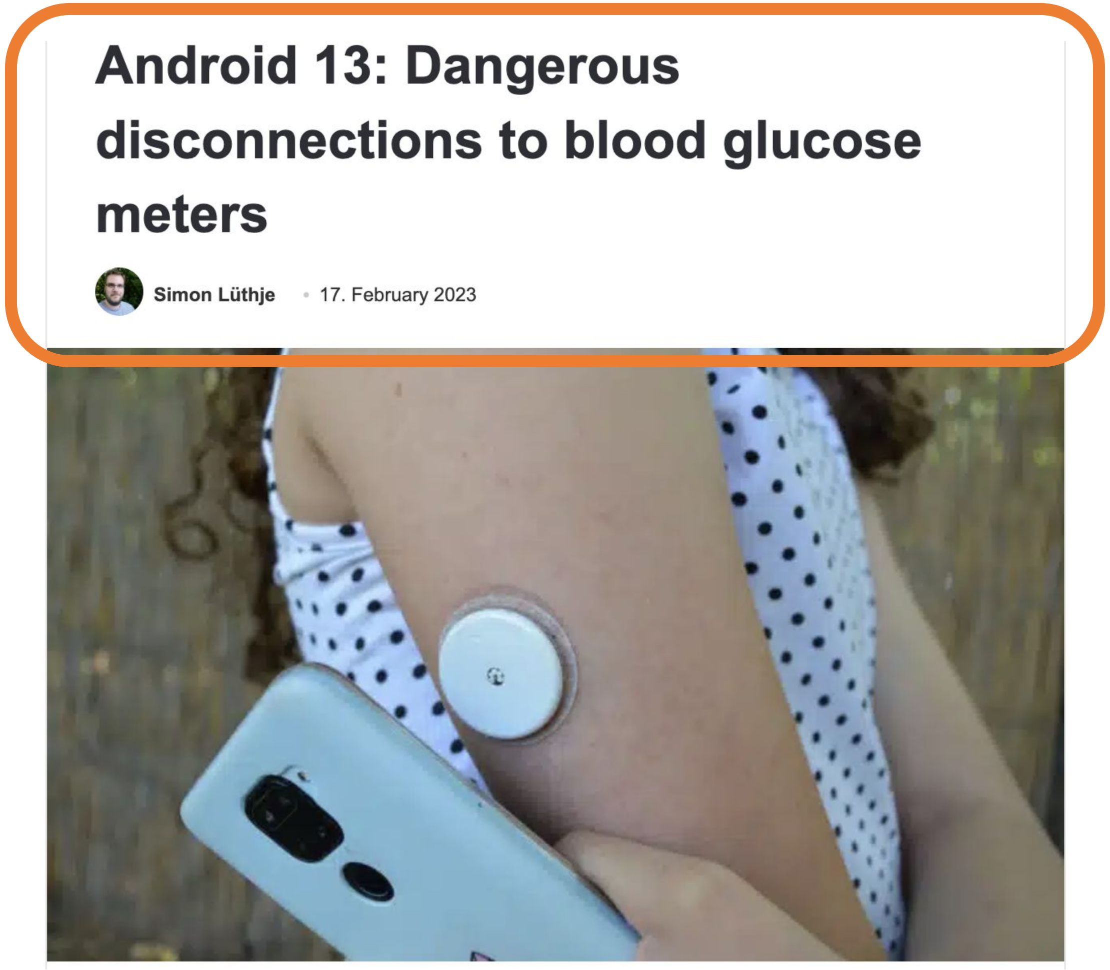
Trusting software is extending agency

- *agency*: our capacity to take actions that align with our goals
- “when we trust, we try to make something a part of our agency... To unquestioningly trust something is to let it in—to attempt to bring it inside one’s practical functioning.”
- Example: glucose monitoring

CT Nguyen: *Trust as an unquestioning attitude*

Risk: Agential Gullibility

- Trusting more than warranted
- Difficult to b/c software changes, hard to inspect
- Example: glucose monitoring issues w/ Android update

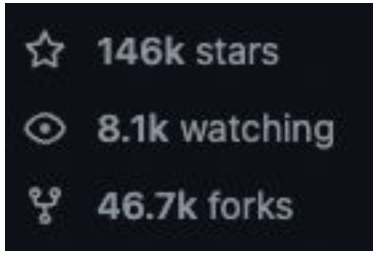


Android 13: Dangerous disconnections to blood glucose meters

Simon Lüthje • 17. February 2023

Three paths to trust

1. Assumption: trust absent any cluses to warrant it
   a. E.g. using unknown third party library b/c deadline nearing
2. Inference: reputation is based on past performance, characteristics, institutions
   a. Some weaker (e.g. trust in brands or affiliation)
   b. Some stronger (e.g. past performance)
   c. Trust in prior versions of software



☆ 146k stars

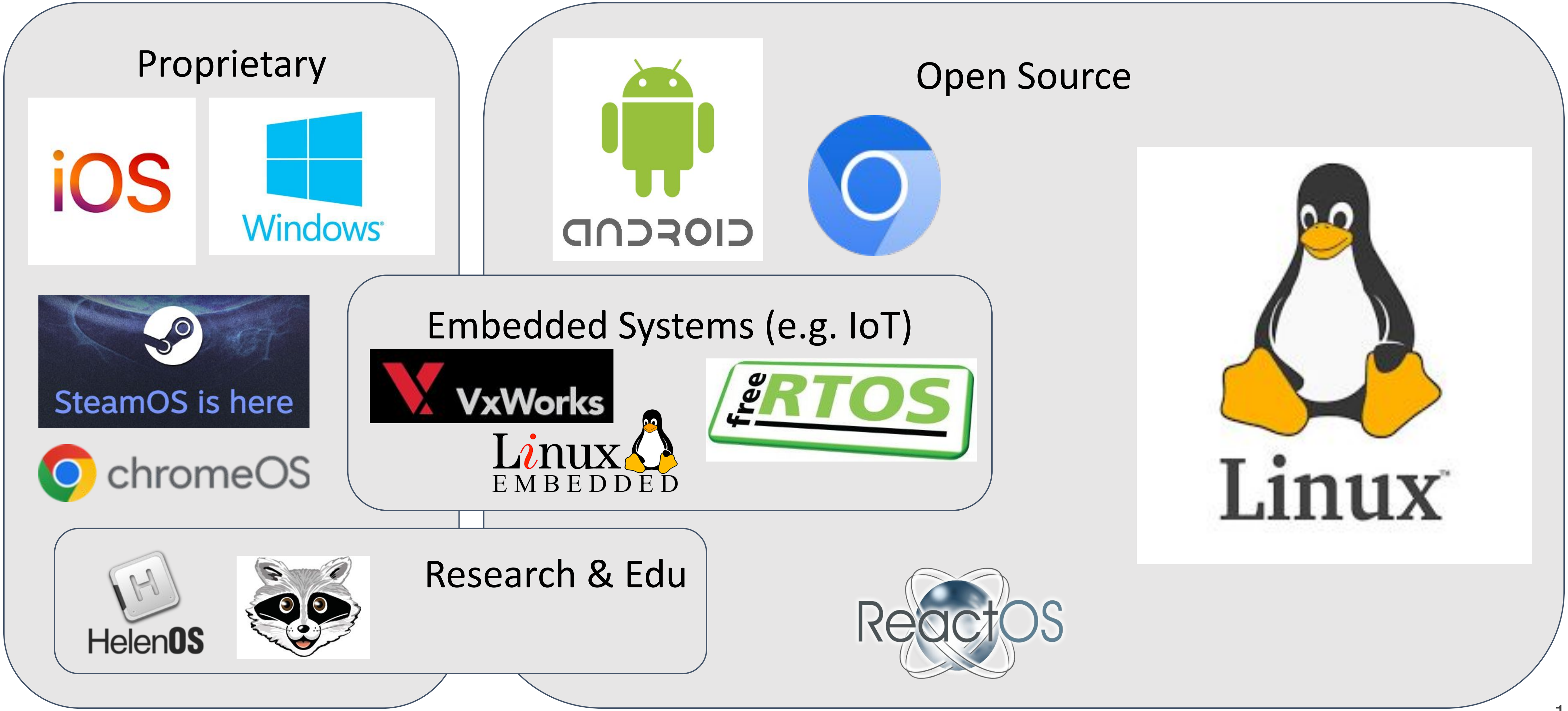
8.1k watching

46.7k forks

3. Substitution: structural arrangements that partly replace need for trust
   a. Often involves separation of code, responsibilities
   b. E.g. user permissions of file system, keeping personal info off work accounts, devices

Paul B. de Laat: *How can contributors to open-source communities be trusted? On the assumption, inference, and substitution of trust*

So many kinds of OS!



Proprietary

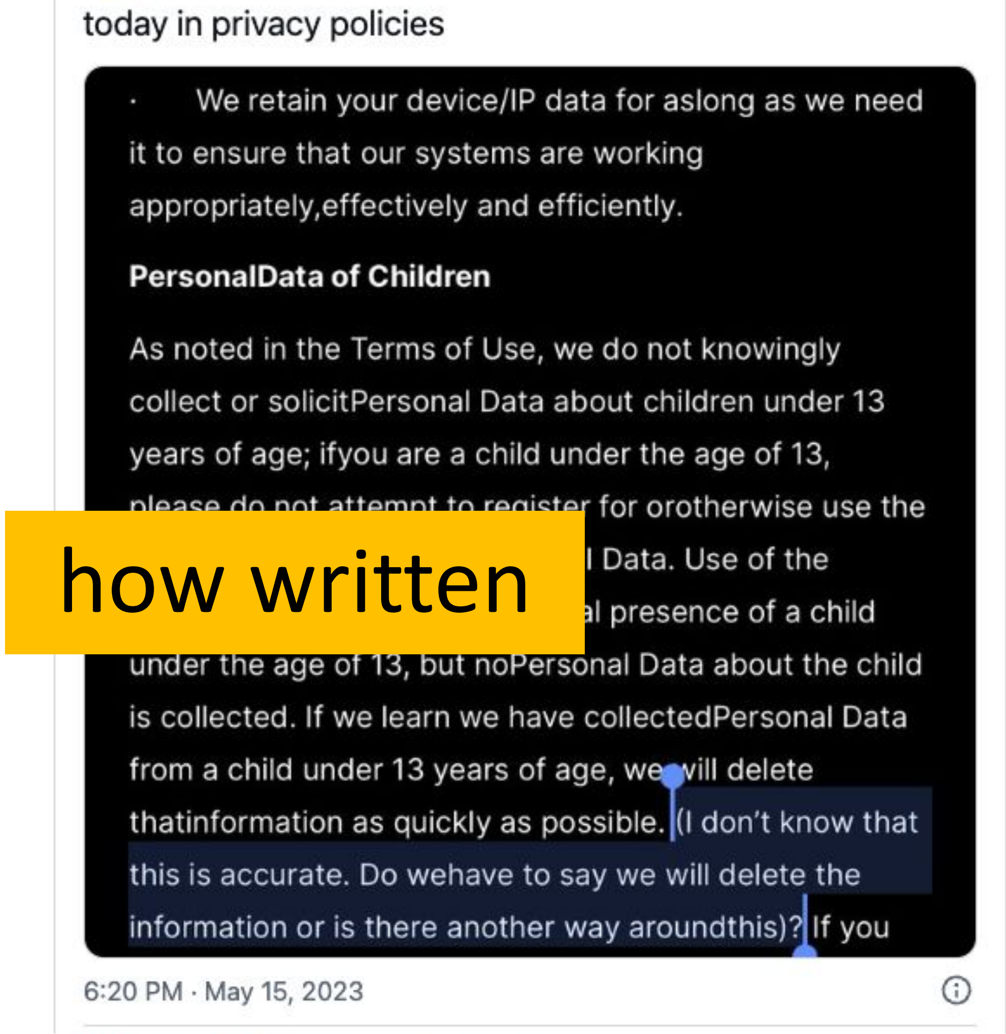
Open Source

Embedded Systems (e.g. IoT)

Research & Edu

As a systems programmer, what is your responsibility as someone designing and maintaining operating systems?

Laws are part of trust (e.g. terms of services)



today in privacy policies

- We retain your device/IP data for aslong as we need it to ensure that our systems are working appropriately,effectively and efficiently.

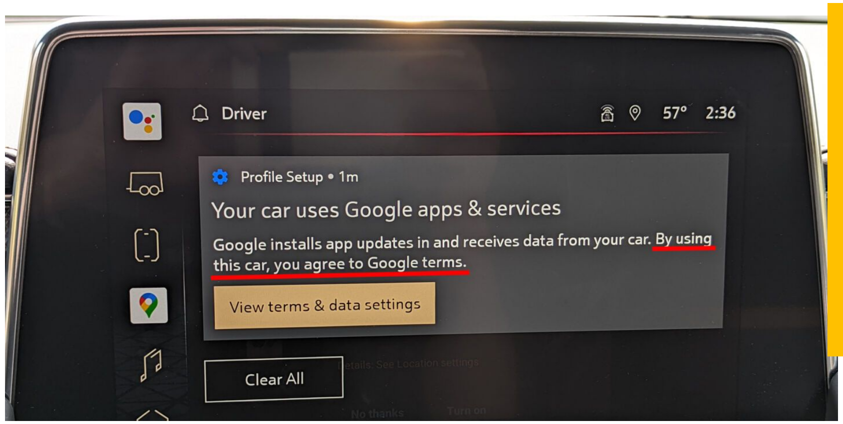
PersonalData of Children

As noted in the Terms of Use, we do not knowingly collect or solicitPersonal Data about children under 13 years of age; ifyou are a child under the age of 13, please do not attempt to register for orotherwise use the … l Data. Use of the … al presence of a child under the age of 13, but noPersonal Data about the child is collected. If we learn we have collectedPersonal Data from a child under 13 years of age, we will delete thatinformation as quickly as possible. (I don't know that this is accurate. Do wehave to say we will delete the information or is there another way aroundthis)? If you

6:20 PM · May 15, 2023

Tech Crunch

how written



Driver 57° 2:36

Profile Setup • 1m

Your car uses Google apps & services

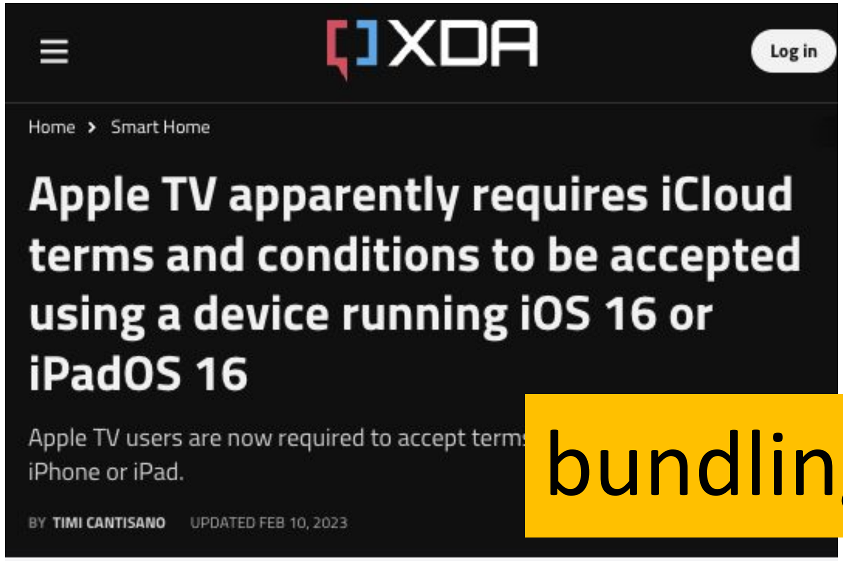
Google installs app updates in and receives data from your car. By using this car, you agree to Google terms.

View terms & data settings

Clear All

ars technica

how informed consent was



Home › Smart Home

Apple TV apparently requires iCloud terms and conditions to be accepted using a device running iOS 16 or iPadOS 16

Apple TV users are now required to accept terms … iPhone or iPad.

BY TIMI CANTISANO UPDATED FEB 10, 2023

bundling

Dimensions of Context

Stakeholders

Types: Direct, indirect
Other considerations: Non-targeted use, changing hands, one person multiple roles

Pervasiveness

How widespread?
For what? (personal, critical infrastructure)
Connected w/ what?
Cultural and political implications?
Crossing national boundaries?

Values

Explicit vs collateral
Value tensions
Different perceptions of same value

Time

Support duration
Obsolescence
Reappropriation

Dimensions of Context

Stakeholders

Types: Direct, indirect
Other considerations: Non-targeted use, changing hands, one person multiple roles

Pervasiveness

How widespread?
For what? (personal, critical infrastructure)
Connected w/ what?
Cultural and political implications?
Crossing national boundaries?

Values

Explicit vs collateral
Value tensions
Different perceptions of same value

Time

Support duration
Obsolescence
Reappropriation

Stakeholders

Direct stakeholders: directly interact w/ system

- users
- app developers
- system programmers

Indirect stakeholders: affected by system w/o directly using it

- customers
- patients
- everyone?!

Additional considerations:

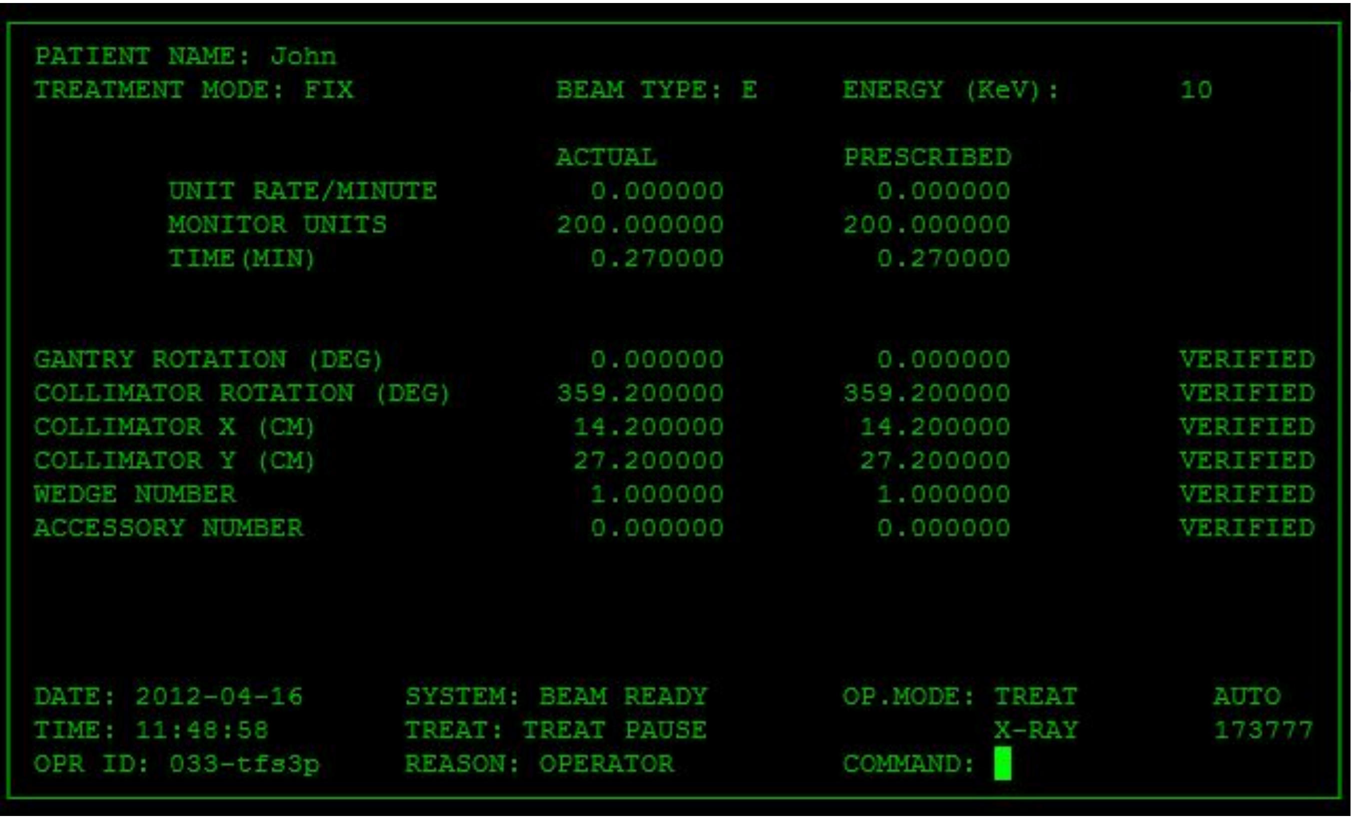
- **non-targeted use**: tech not always used the way designers intended
- **changing hands**: stewardship of OS handed off between systems or organizations
- **one person, multiple roles**: same person can be direct and indirect stakeholder

Example: Therac 25

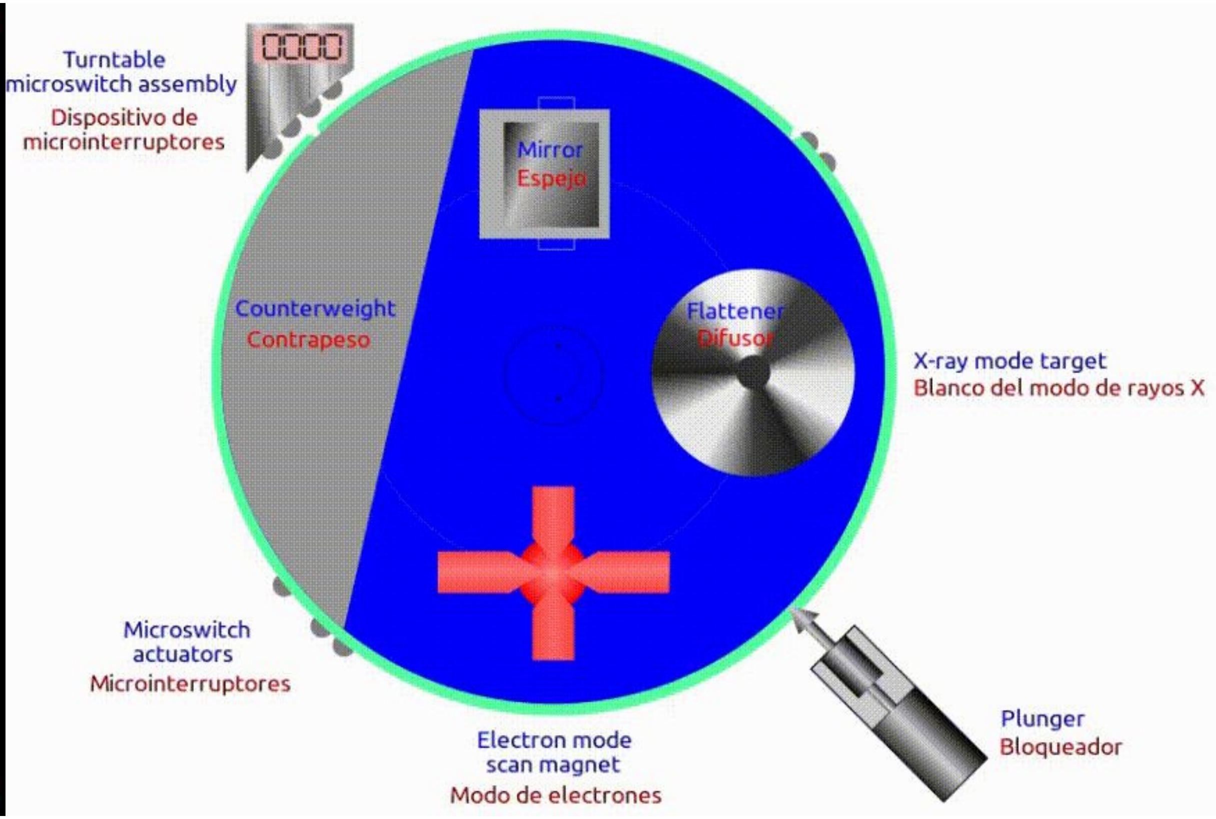
- Radiation therapy machine
- 1985-87: 6 patient deaths (overdoses of radiation)
- dual-mode: switch between by
  - low energy electron: topical cancer
  - high energy X-ray beams: deep cancers

Therac-6	Therac-20	Therac-25
- Photon-mode - Manual device - Hardware safety features	**- Dual-mode** - Manual device - Hardware safety features - Hardware interlocks prevented accidents from occuring	- Dual-mode **- Automatic device** **- Some hardware safety features replaced with software**

Race condition in Therac-25



```
PATIENT NAME: John
TREATMENT MODE: FIX              BEAM TYPE: E      ENERGY (KeV):         10

                                 ACTUAL            PRESCRIBED
        UNIT RATE/MINUTE           0.000000          0.000000
        MONITOR UNITS            200.000000        200.000000
        TIME(MIN)                  0.270000          0.270000


GANTRY ROTATION (DEG)              0.000000          0.000000            VERIFIED
COLLIMATOR ROTATION (DEG)        359.200000        359.200000            VERIFIED
COLLIMATOR X (CM)                 14.200000         14.200000            VERIFIED
COLLIMATOR Y (CM)                 27.200000         27.200000            VERIFIED
WEDGE NUMBER                       1.000000          1.000000            VERIFIED
ACCESSORY NUMBER                   0.000000          0.000000            VERIFIED




DATE: 2012-04-16      SYSTEM: BEAM READY         OP.MODE: TREAT          AUTO
TIME: 11:48:58        TREAT: TREAT PAUSE                  X-RAY          173777
OPR ID: 033-tfs3p     REASON: OPERATOR           COMMAND: █
```



Not considering context, poor SWE

Poor software engineering practices

1. all code written by single programmer
2. no formal software specifications
3. no testing strategy
4. no external review
5. uninformative error messages

Failure to consider stakeholders:

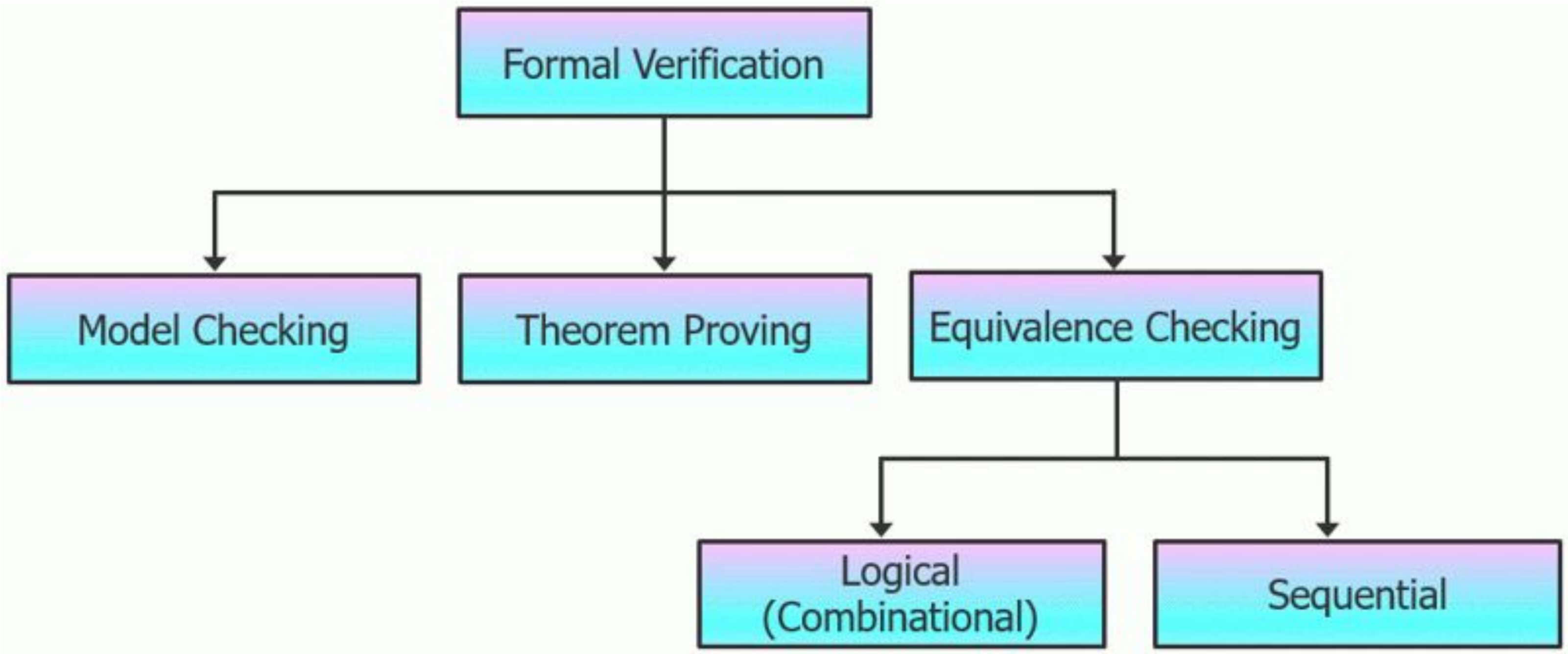
Direct stakeholders: medical technician, programmer, service technician

Indirect stakeholders: patients

Non-targeted use: technicians worked too quickly

Changing hands: used buggy software from previous versions (which had redundant hardware safety)

Modern medical software undergo formal verification



Aijaz Fatima

Dimensions of Context

Stakeholders (direct, indirect)

Types: Direct, indirect
Other considerations: Non-targeted use, changing hands, one person multiple roles

Pervasiveness

How widespread?
For what? (personal, critical infrastructure)
Connected w/ what?
Cultural and political implications?
Crossing national boundaries?

Values

Explicit vs collateral
Value tensions
Different perceptions of same value

Time

Support duration
Obsolescence
Reappropriation

Pervasiveness

- How widespread is use?
- For what? (personal, recreation, critical infrastructure)
- Crossing national boundaries (different rules, customs, infrastructure)?
- Connected w/ what?
- Cultural and political implications?

Dimensions of Context

Stakeholders

Types: Direct, indirect
Other considerations: Non-targeted use, changing hands, one person multiple roles

Pervasiveness

How widespread?
For what? (personal, critical infrastructure)
Connected w/ what?
Cultural and political implications?
Crossing national boundaries?

Values

Explicit vs collateral
Value tensions
Different perceptions of same value

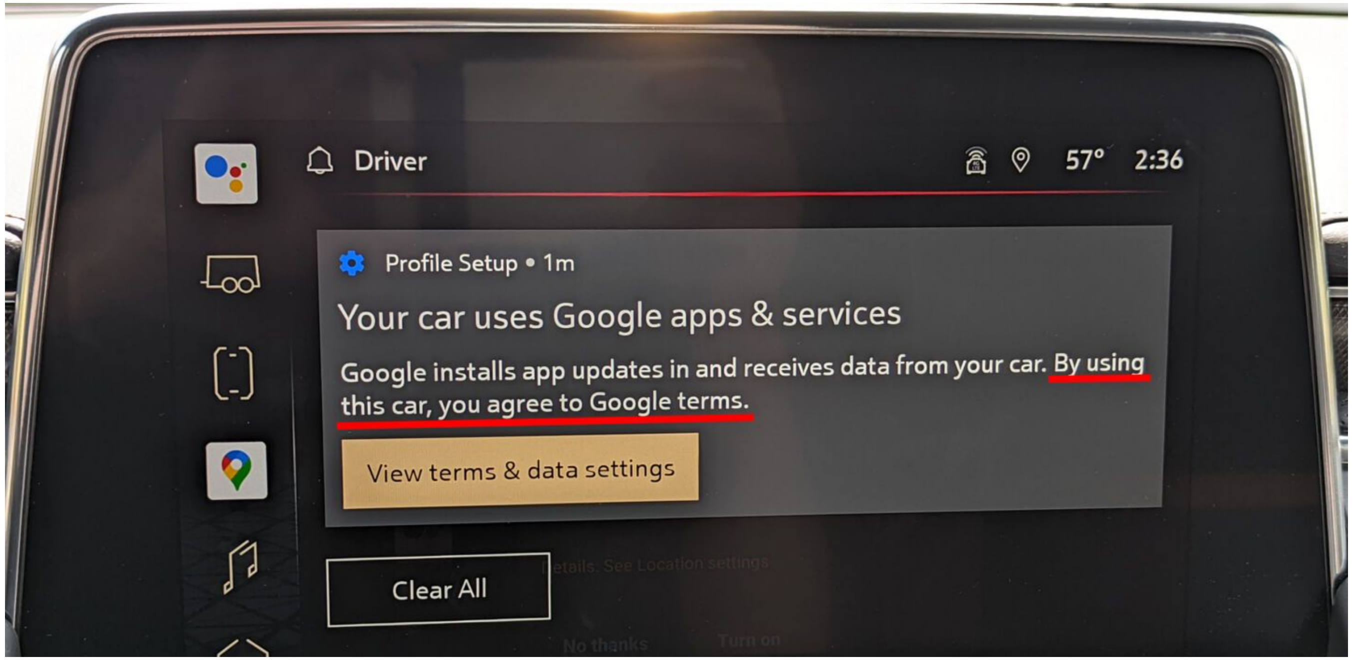
Time

Support duration
Obsolescence
Reappropriation

Values

- Explicit values: values designers intended to design for
- Collateral values: side effects of design decisions
- Value tensions: one value in a technology challenges another value
- Perceptions of a value: stakeholders have different perceptions of definition of a specific value
  - e.g. privacy as control over own information vs being left alone

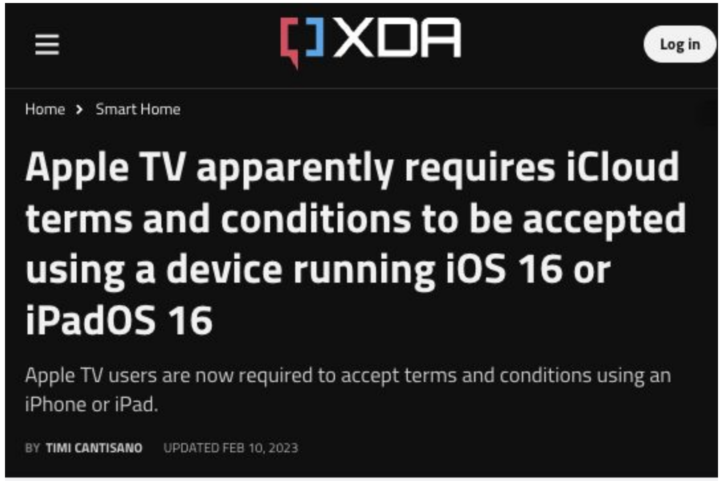
Bundling: A growing value tension



Profile Setup • 1m

Your car uses Google apps & services

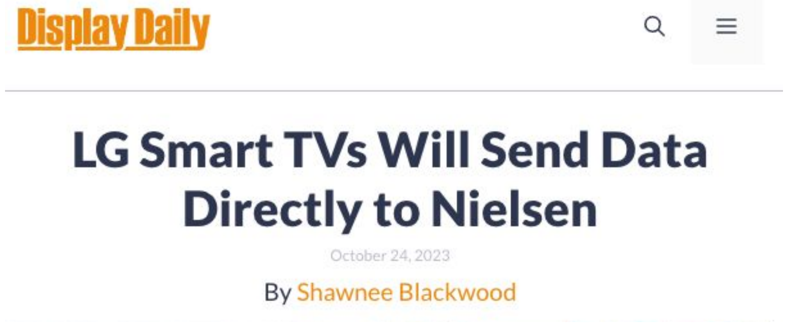
Google installs app updates in and receives data from your car. By using this car, you agree to Google terms.



Apple TV apparently requires iCloud terms and conditions to be accepted using a device running iOS 16 or iPadOS 16

Apple TV users are now required to accept terms and conditions using an iPhone or iPad.

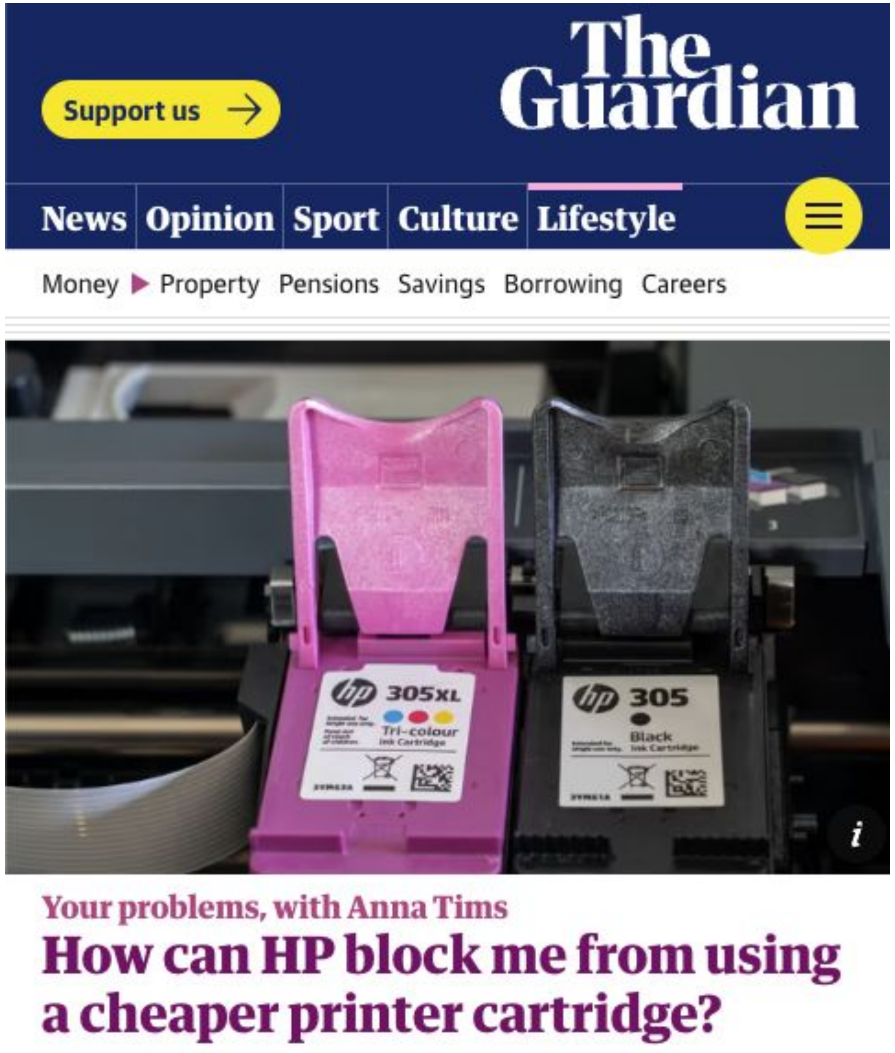
BY TIMI CANTISANO UPDATED FEB 10, 2023



LG Smart TVs Will Send Data Directly to Nielsen

October 24, 2023

By Shawnee Blackwood

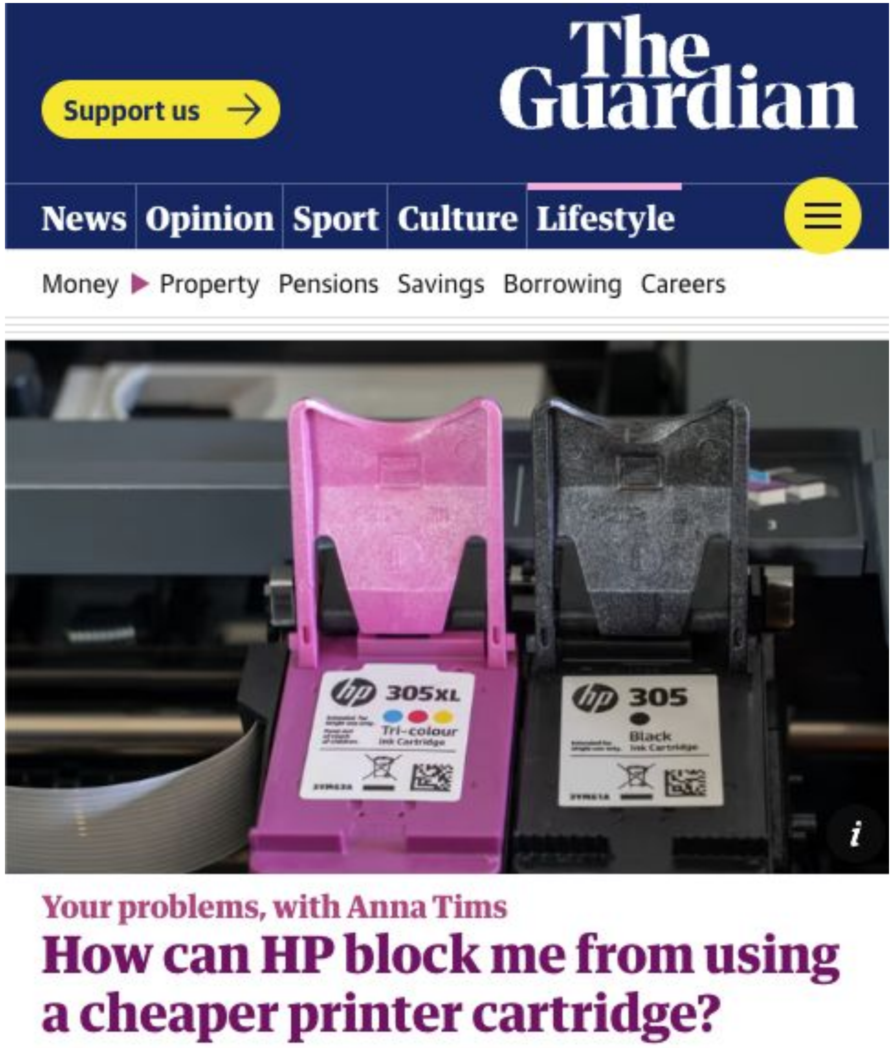


Your problems, with Anna Tims

How can HP block me from using a cheaper printer cartridge?

Bundling: A growing value tension

- Printers preventing use of cartridges from other manufacturers
- HP customer support: “purpose of dynamic security feature is to protect HP’s innovations and intellectual property”
- included in security updates
- **explicit values**: security
- **collateral values**: profit, quality,
- **value tension**: (lack of) sustainability
- **perceptions of values**: network security vs security of intellectual property



Your problems, with Anna Tims

How can HP block me from using a cheaper printer cartridge?

Dimensions of Context

Stakeholders

Types: Direct, indirect
Other considerations: Non-targeted use, changing hands, one person multiple roles

Pervasiveness

How widespread?
For what? (personal, critical infrastructure)
Connected w/ what?
Cultural and political implications?
Crossing national boundaries?

Values

Explicit: intentionally designed for (e.g. privacy, trust, adaptability, performance)?

Collateral: side effects of design decisions

Time

Support duration
Obsolescence
Reappropriation

Dimensions of Context

Stakeholders

Types: Direct, indirect
Other considerations: Non-targeted use, changing hands, one person multiple roles

Pervasiveness

How widespread?
For what? (personal, critical infrastructure)
Connected w/ what?
Cultural and political implications?
Crossing national boundaries?

Values

Explicit vs collateral
Value tensions
Different perceptions of same value

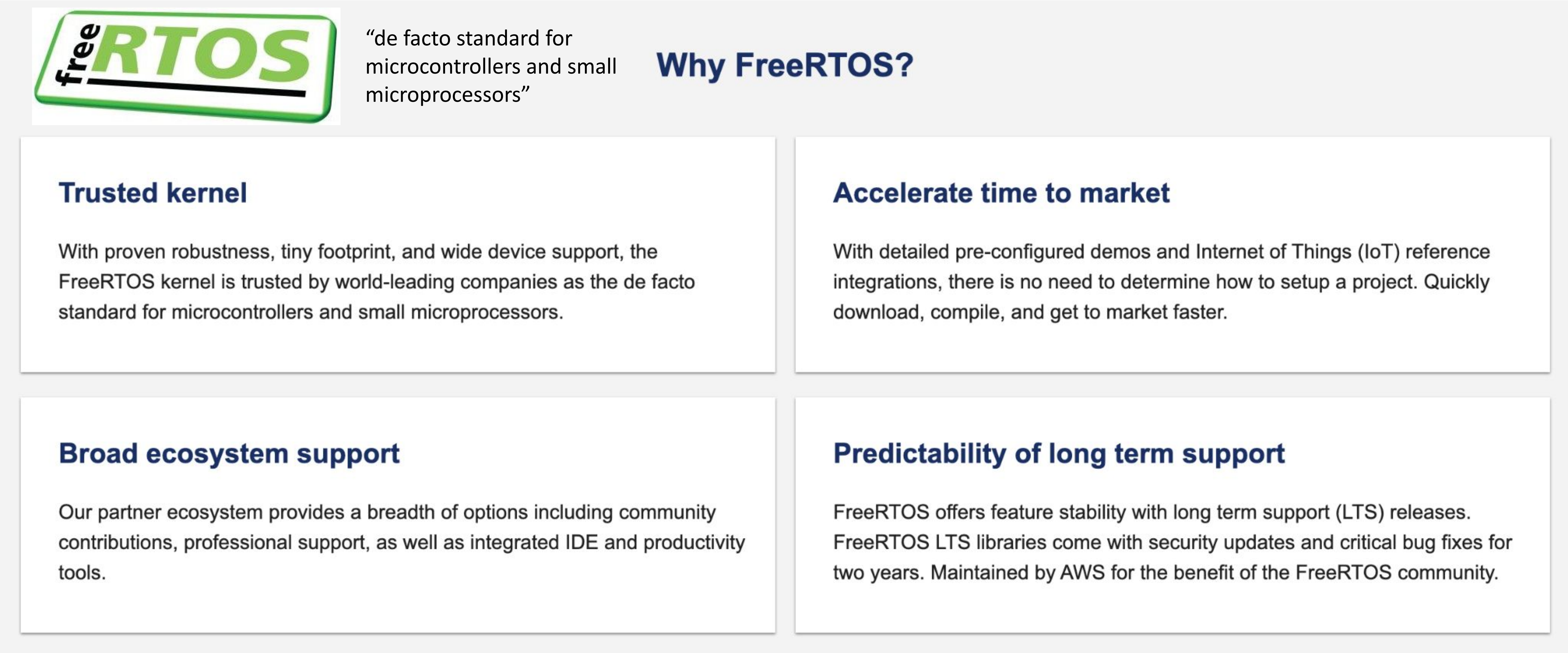
Time

Support duration
Obsolescence
Reappropriation

Time

- Support duration (long-term support)
- Obsolescence: manage end of support?
- Reappropriation: how OS reappropriated in novel way?
- Choice not to use (or stop using)?

FreeRTOS communicating trust



“de facto standard for microcontrollers and small microprocessors”

Why FreeRTOS?

Trusted kernel

With proven robustness, tiny footprint, and wide device support, the FreeRTOS kernel is trusted by world-leading companies as the de facto standard for microcontrollers and small microprocessors.

Accelerate time to market

With detailed pre-configured demos and Internet of Things (IoT) reference integrations, there is no need to determine how to setup a project. Quickly download, compile, and get to market faster.

Broad ecosystem support

Our partner ecosystem provides a breadth of options including community contributions, professional support, as well as integrated IDE and productivity tools.

Predictability of long term support

FreeRTOS offers feature stability with long term support (LTS) releases. FreeRTOS LTS libraries come with security updates and critical bug fixes for two years. Maintained by AWS for the benefit of the FreeRTOS community.

The original smartwatch… lives?

Kicking a Pebble (OS) down the road…

pebble

2012: Raised $10.3 million on Kickstarter

2015: Pebble raises $20.3 mil from 75k backers on Kickstarter

2016: Pebble company shut down, IP sold to Fitbit

2016: Rebble community founded

2018: official Pebble support ended

Pebble OS (proprietary, built upon FreeRTOS)

freeRTOS

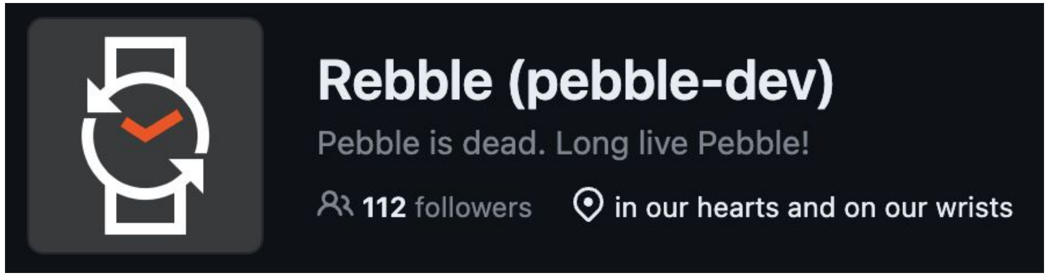
“de facto standard for microcontrollers and small microprocessors”

2017: Rebble Alliance founded, creates RebbleOS

pebble-dev / RebbleOS

Pebble is dead! Long live Pebble!

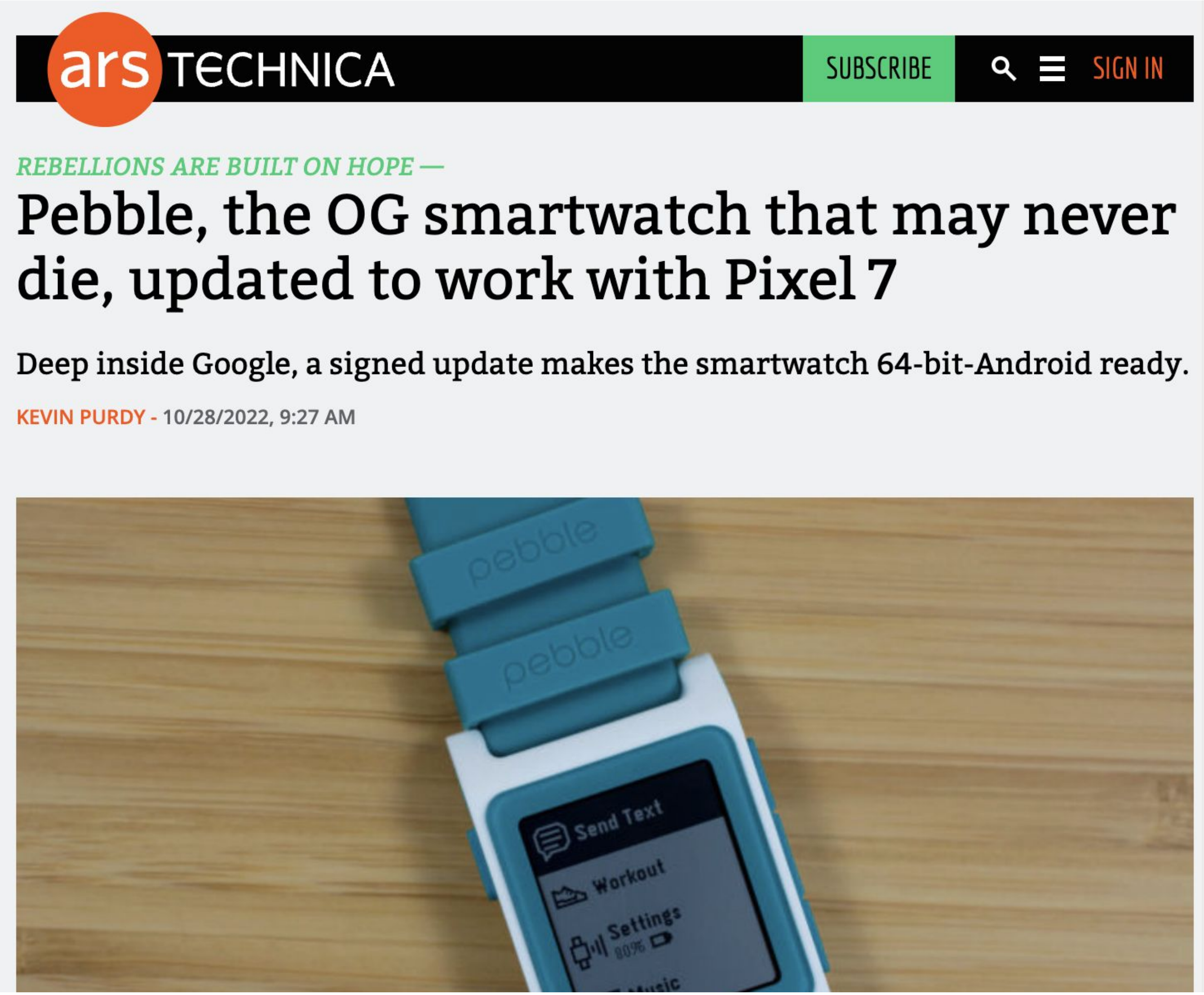
- 2021: Fitbit acquired by Google
- 2021: Pebble app removed from iOS App Store
- 2022: New Pebble Android app (for 64 bit only Android OS)
  - signed w/ official Pebble keys



Rebble (pebble-dev)

Pebble is dead. Long live Pebble!

112 followers · in our hearts and on our wrists



REBELLIONS ARE BUILT ON HOPE —

Pebble, the OG smartwatch that may never die, updated to work with Pixel 7

Deep inside Google, a signed update makes the smartwatch 64-bit-Android ready.

KEVIN PURDY - 10/28/2022, 9:27 AM

Dimensions of Context

Stakeholders

Types: Direct, indirect
Other considerations: Non-targeted use, changing hands, one person multiple roles

Pervasiveness

How widespread?
For what? (personal, critical infrastructure)
Connected w/ what?
Cultural and political implications?
Crossing national boundaries?

Values

Explicit vs collateral
Value tensions
Different perceptions of same value

Time

Support duration
Obsolescence
Reappropriation

Trust and OS in Context

1. Trust amongst tech **users, app developers, and system programmers** is intertwined
2. Trust is about **extending agency** (“unquestioning attitude”)
3. Trust emerges through **assumption, inference, substitution**
4. Can **design ways to substitute** some need to trust

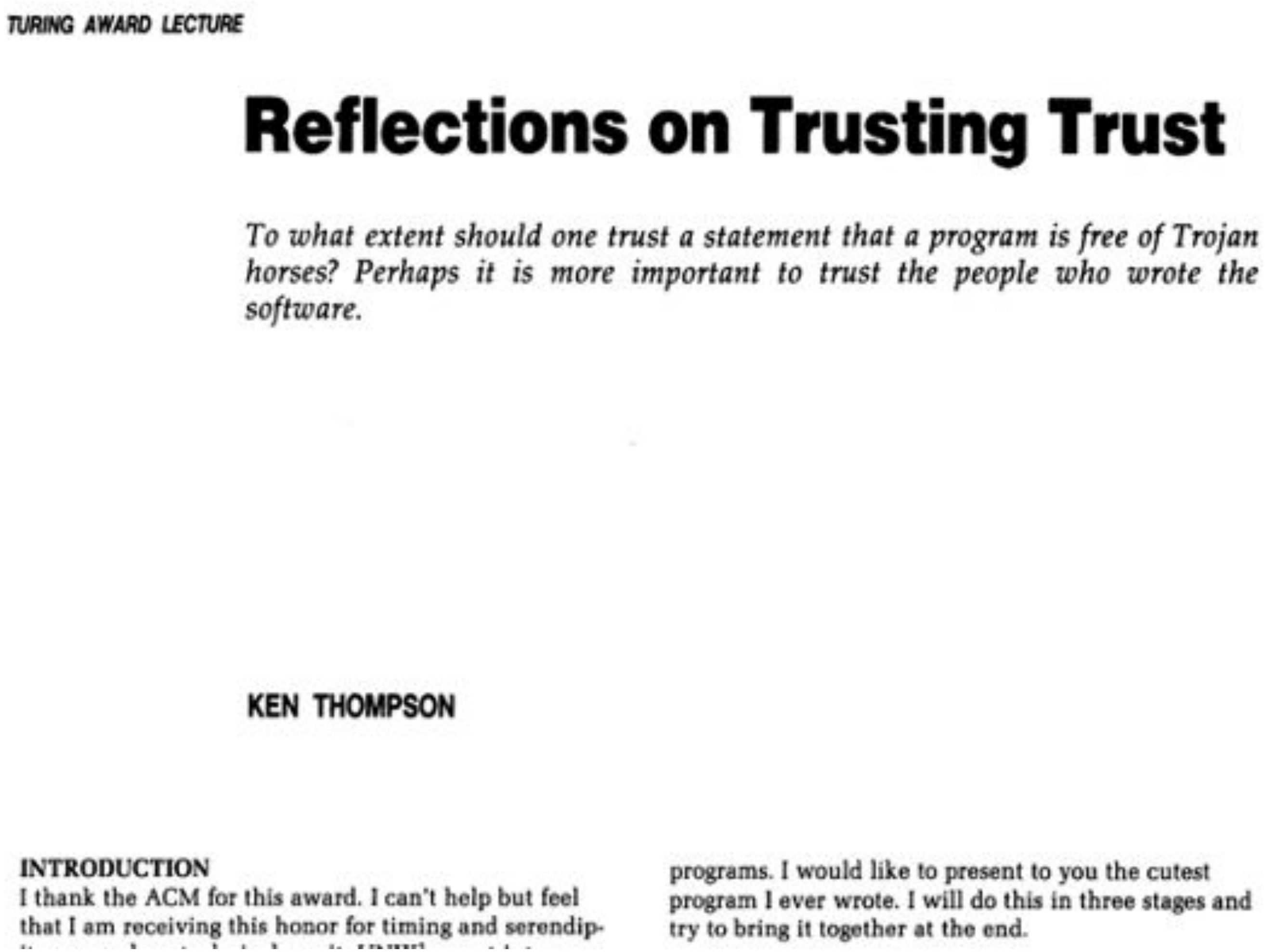
Stakeholders
Direct & indirect, Non-targeted use, changing hands, one person multiple roles

Pervasiveness: How widespread? For what? Connected w/ what? Cultural, political, national boundaries

Values
Explicit vs collateral, value tensions, Different perceptions of same value

Time
Support duration, obsolescence, reappropriation

Trusting systems involves trusting people



TURING AWARD LECTURE

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

INTRODUCTION
I thank the ACM for this award. I can't help but feel that I am receiving this honor for timing and serendip-

programs. I would like to present to you the cutest program I ever wrote. I will do this in three stages and try to bring it together at the end.

Thompson, Ken. "Reflections on trusting trust." Communications of the ACM 27.8 (1984): 761-763.

Trust and OS in Context

1. Trust amongst tech **users, app developers, and system programmers** is intertwined
2. Trust is about **extending agency** ("unquestioning attitude")
3. Trust emerges through **assumption, inference, substitution**
4. Can **design ways to substitute** some need to trust

Stakeholders
Direct & indirect, Non-targeted use, changing hands, one person multiple roles

Pervasiveness: How widespread? For what? Connected w/ what? Cultural, political, national boundaries

Values
Explicit vs collateral, value tensions, Different perceptions of same value

Time
Support duration, obsolescence, reappropriation

Benjamin Xie, Ph.D. | Embedded Ethics Fellow | benjixie@stanford.edu | benji.phd