

Wrap-up

Information Privacy with Applications

David Sidi (dsidi@email.arizona.edu)



Administrative

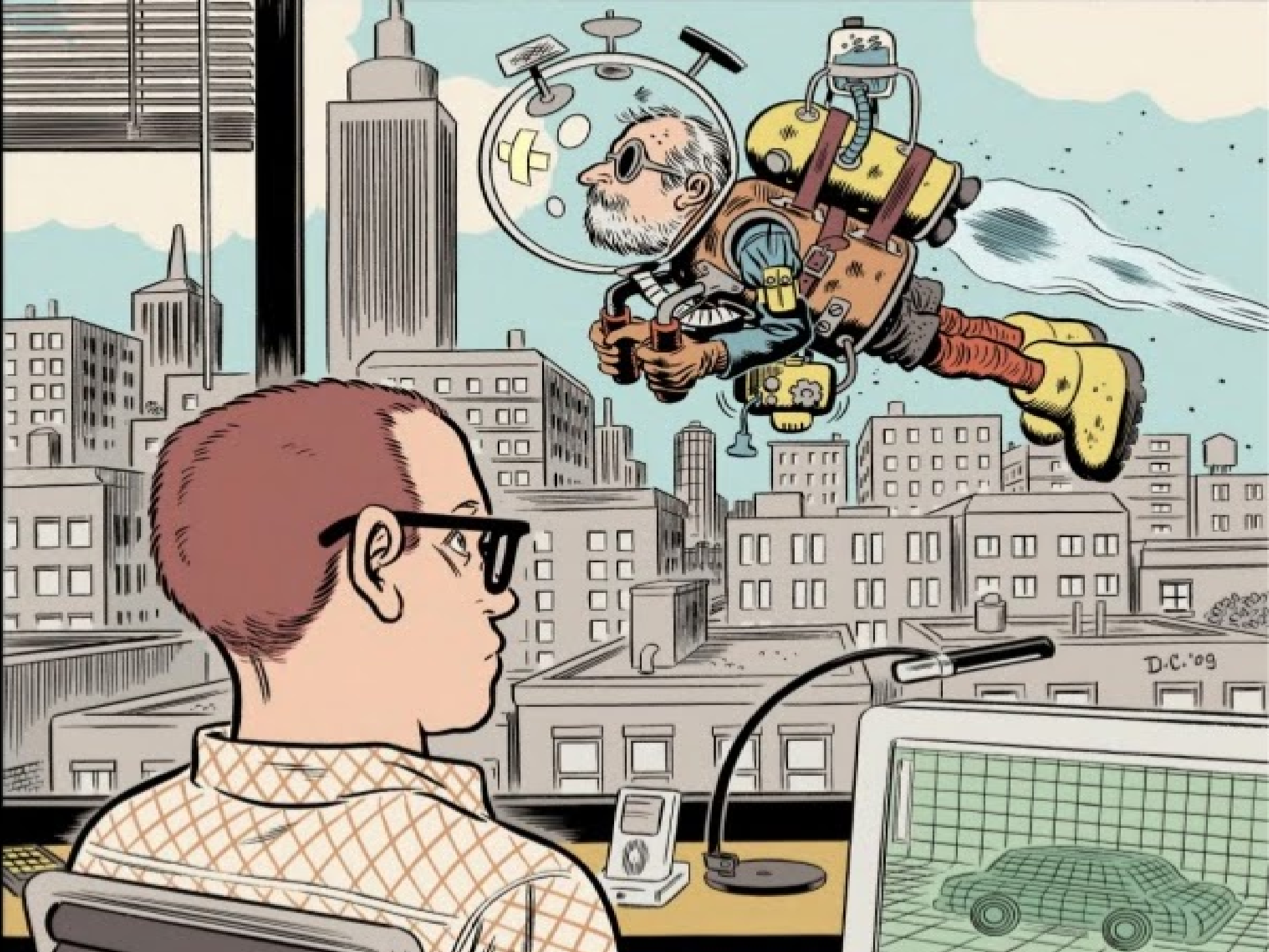
- Get everything that is still outstanding turned in!

Learning
how to
learn



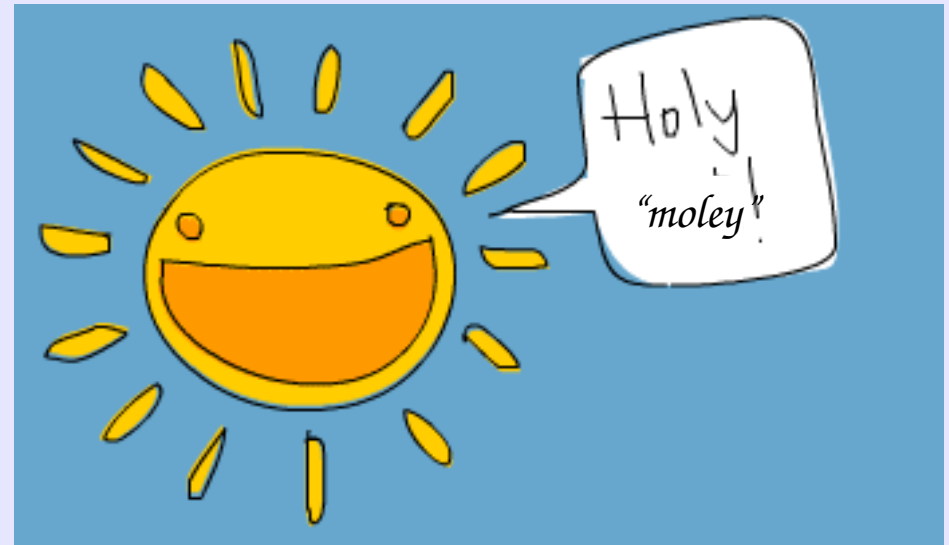
Any type ▾





Every darn thing

- recognize security problems
- set up a server for your own purposes
- set up an onion service
- countermeasures to standoff biometry
- building trust rationally
- learn a cryptographic primitive that is new to you, and implement it





More on this

- [shell scripting](#) with Korn Shell
- [setting up OpenBSD](#)
- [Shellcoder's handbook](#)
- [Set up a VPN for yourself](#)
- [Do some cryptanalysis](#)



Nest
Google Wallet Gmail
Slides
Google Analytics Books
Chromecast
Google+ Maps AdSense
Drive
Sheets Android
Google News Pixel
ChromeOS
DNS Calendar Chrome Allo
PRISM Home Duo
Google Wifi
Docs DeepMind
YouTube Search Photos
Translate
Google Fiber
Keep

it's fiiiiiiiiine

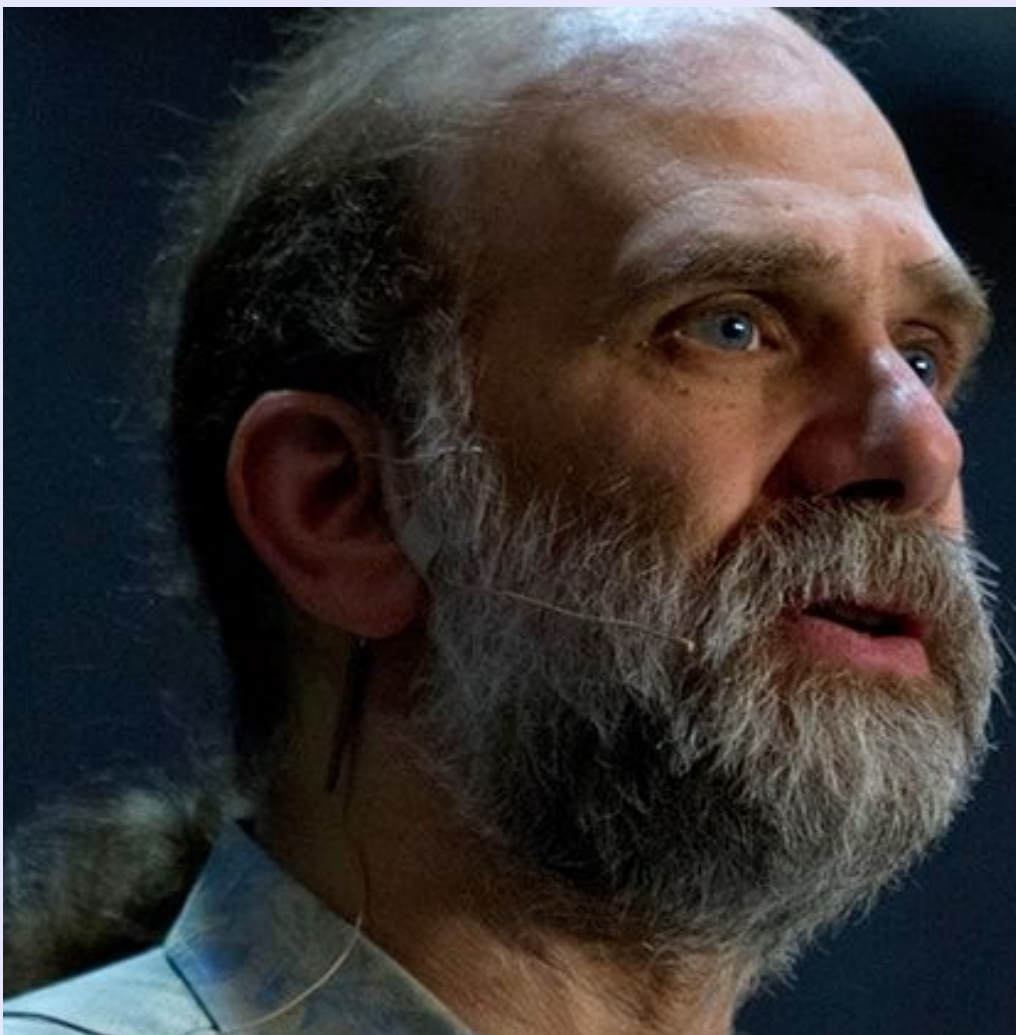


Maciej Cegłowski, Haunted by Data

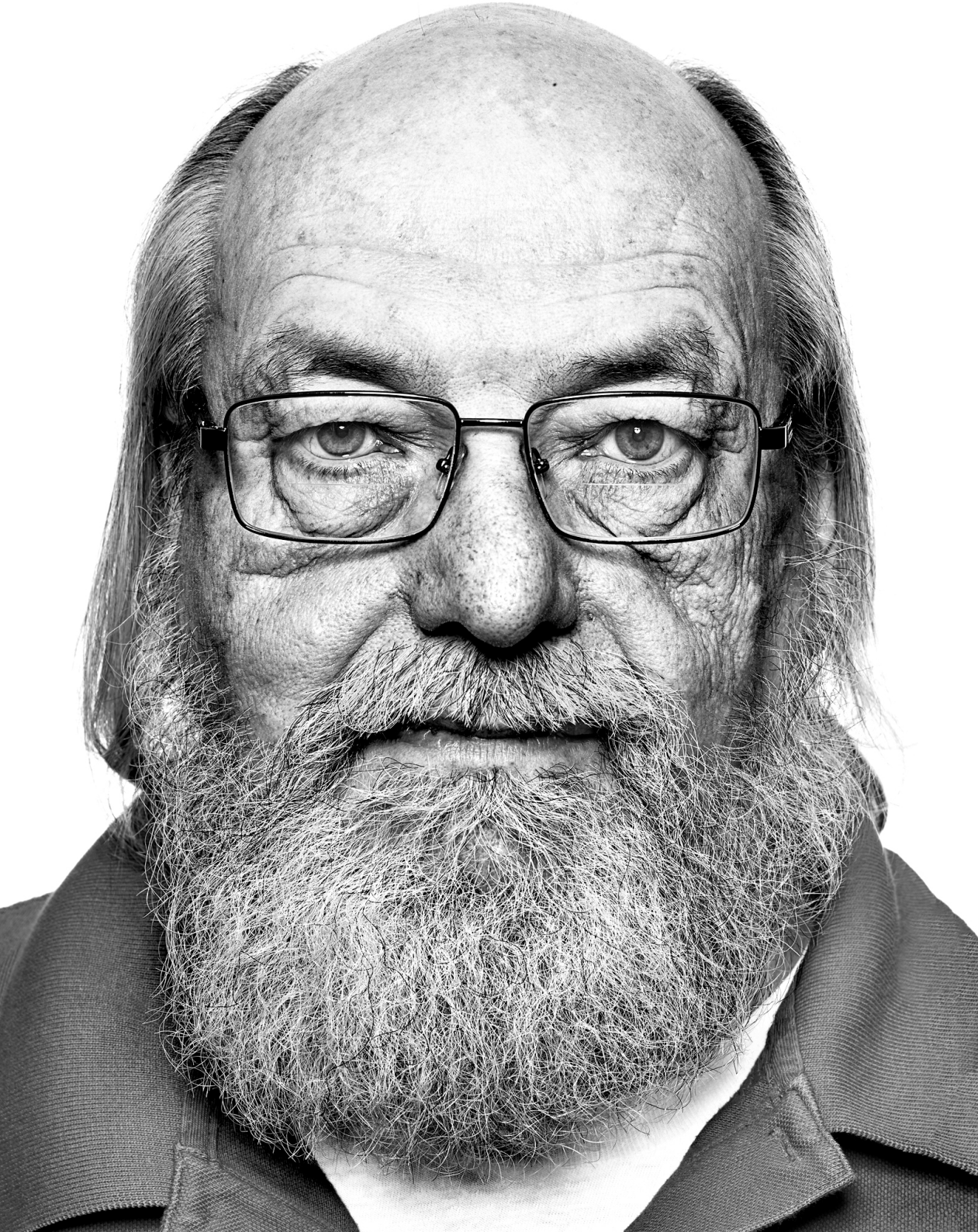
A photograph of John Abelson, a man with thinning brown hair, wearing a dark blue blazer over a light blue button-down shirt. He is speaking and gesturing with his right hand, palm facing forward. A small black lavalier microphone is clipped to his shirt. The background is dark and out of focus.

“A computational process is indeed much like a sorcerer’s idea of a spirit. It cannot be seen or touched. It is not composed of matter at all. However, it is very real. It can perform intellectual work. It can answer questions. It can affect the world by disbursing money at a bank or by controlling a robot arm in a factory. The programs we use to conjure processes are like a sorcerer’s spells.”

Abelson, SICP

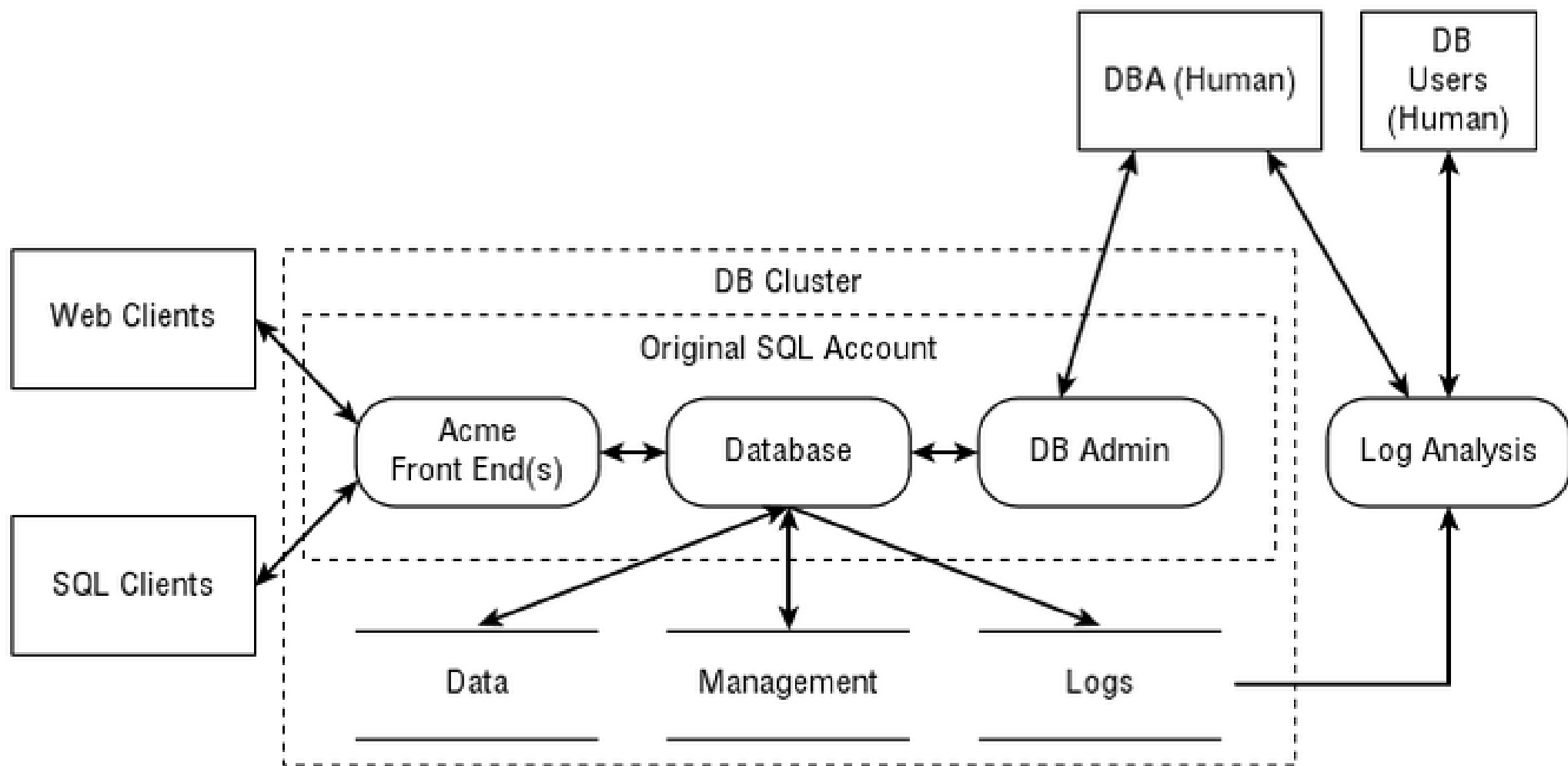


“We already knew that technology can subvert law. Snowden demonstrated that law can also subvert technology. Both fail unless each work. It's not enough to just let technology do its thing.”



The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me). No amount of source-level verification or scrutiny will protect you from using untrusted code.

Ken Thompson, ACM Turing Award Speech, "Reflections on Trusting Trust"



Key:



Figure 2-4: A modern DFD model (previously shown as Figure 2-1)

“...[the] *moral decision* to tell the public about spying that affects all of us has been costly, but it was the right thing to do and I have no regrets.”
[emph. added]

- Edward Snowden





Week

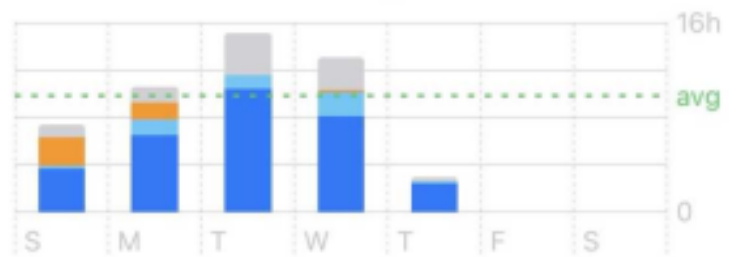
Day

SCREEN TIME

Daily Average

9h 48m

↑ 28% from last week



Social
30h 57m

Entertainment
5h 2m

Travel
3h 56m

Total Screen Time

49h 4m

Updated today at 8:51 AM

MOST USED

[SHOW CATEGORIES](#)



WhatsApp

10h 42m

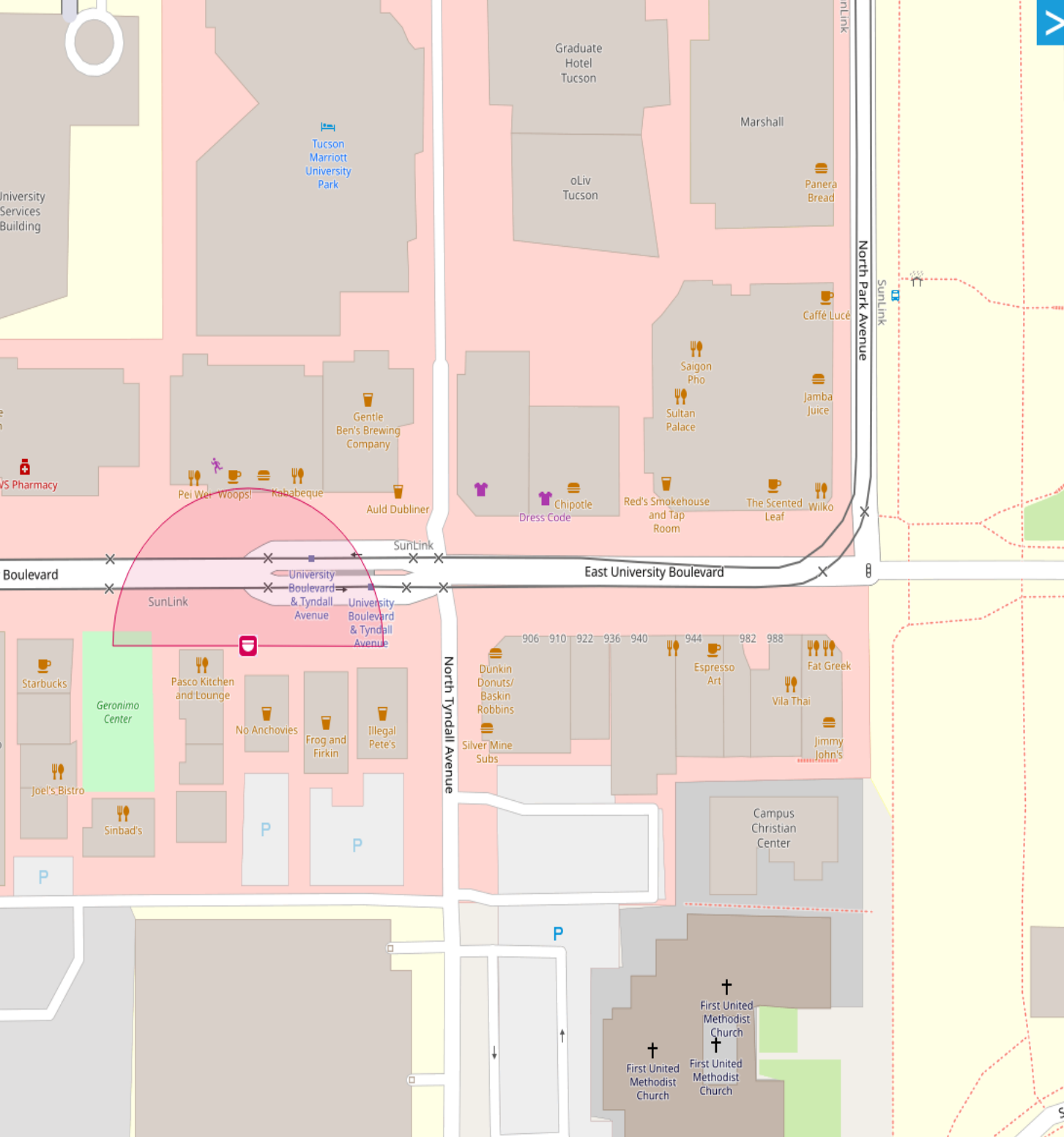


Snapchat

8h 58m



Twitter



Surveillance under Surveillance

what this is about

Surveillance under Surveillance shows you cameras and guards — watching you — almost everywhere. You can see where they are located and, if the information is available, what type they are, the area they observe, or other interesting facts.

Different icons and colors give you a quick overview about the indexed surveillance entries. Click on those icons on the map to get the available information.

Icons



Camera — no further information



Fixed camera — usually observing a limited area



Panning camera — usually able to observe various areas

Demographics microdata is private and can lead to serious harm, so it can't be released to the public.

On the other hand, some of the benefits of that microdata can be had *only* if they or their products are released to the public.

So we need a way to release statistical tables that resists attempts to infer the underlying microdata from the statistics.



attributes

records

	Name	Age	Race	Marital Status
1	Jane Doe	37	White	Single
2	Joe Bloggs	40	Black	Married

MICRODATA TABLE

statistic	group	count	median	mean
1A	total population	7	37	35
2A	female	4	39.5	41
2B	male	3	25	27
2C	black or African American	3	40	48
2D	white	4	26.5	25.25
3A	single adults	(D)	(D)	(D)
3B	married adults	4	38.5	45.25
4A	black or African American male	(D)	(D)	(D)
4B	black or African American female	(D)	(D)	(D)
4C	white male	(D)	(D)	(D)
4D	white female	(D)	(D)	(D)
5A	persons under 5 years	(D)	(D)	(D)
5B	persons under 18 years	(D)	(D)	(D)
5C	persons 64 years or over	(D)	(D)	(D)

STATISTICAL TABLE

```

c 1 Writing map file : /tmp/sugar10907.map
c 1 Heap : 5 MiB used (max 241 MiB), NonHeap : 6 MiB used (max 0 MiB)
c 1 SAT : 5851 SAT variables, 186151 SAT clauses, 3267684 bytes
c 1 Heap : 5 MiB used (max 241 MiB), NonHeap : 6 MiB used (max 0 MiB)
c 1 ENCODING CPU 0.98 (0 0 0.91 0.07)
c 1 SOLVING /tmp/sugar10907.cnf WITH /tmp/sugar10907.map
c 1 SAT SOLVING /tmp/sugar10907.cnf
c 1 CMD minisat '/tmp/sugar10907.cnf' '/tmp/sugar10907.out'
c 1 WARNING: for repeatability, setting FPU to use double precision
c 1 =====[ Problem Statistics ]=====
c 1 |
c 1 |   Number of variables:      5851
c 1 |   Number of clauses:      186139
c 1 |   Parse time:              0.04 s
c 1 |   Eliminated clauses:      0.03 Mb
c 1 |   Simplification time:     0.22 s
c 1 |
c 1 =====[ Search Statistics ]=====
c 1 | Conflicts |      ORIGINAL      |   LEARNT   | Progress |
c 1 |           | Vars  Clauses Literals |   Limit  Clauses Lit/Cl |   |
c 1 |=====|=====|=====|=====|
c 1 restarts      : 1
c 1 conflicts     : 32          (123 /sec)
c 1 decisions     : 51          (0.00 % random) (196 /sec)
c 1 propagations  : 26464       (101785 /sec)
c 1 conflict literals : 213      (20.52 % deleted)
c 1 Memory used   : 34.00 MB
c 1 CPU time      : 0.26 s
c 1
c 1 SATISFIABLE
c 1 DECODING /tmp/sugar10907.out WITH /tmp/sugar10907.map
c 1 CMD java -cp '/usr/local/lib/sugar/sugar-2.3.4.jar' jp.kobe_u.sugar.SugarMain -v -v -decode '/tmp/sugar10907.out' '/tmp/sugar10907.map'
c 1      ing /tmp/sugar10907.out

```

```

s SATISFIABLE

```

```

a S1 0
a S2 1
a S3 1
a S4 0
a S5 1
a S6 0
a S7 0
a A1 6
a A2 16
a A3 25
a A4 37
a A5 40
a A6 42
a A7 79
a R1 1
a R2 1
a R3 0
a R4 1
a R5 0
a R6 1
a R7 0
a M1 0
a M2 0
a M3 1
a M4 1
a M5 1
a M6 0
a M7 1

```


[Course Home](#) [Content](#) [Assignments](#) [Discussions](#) [Quizzes](#) [Grades](#) [Classlist](#) [UA Tools](#) [Library Tools](#) [Course Admin](#) [More](#)

[Manage Quizzes](#) [Question Library](#) [Statistics](#) [LockDown Browser](#)

[Help](#)

[New Quiz](#) [Edit Categories](#) [More Actions](#)

View: [By Category](#) [Apply](#)

[Bulk Edit](#)

☐	Without Category	Published
☐	PhonyTest- Requires Respondus LockDown Browser	-

