Who’s secure, who’s not, & who makes that choice.

•••

Maddie Stone
AppSec Village Keynote 2020

@maddiestone (she/her)

- Security researcher on Google Project Zero
    - Focused on 0-days exploited in the wild
- Previously, Security engineer on Google Play Protect within Android Security at Google
    - Focused on pre-installed and non-Google Play store apps
- Reverse engineer all the things.
- Knows every word in Hamilton

Who’s secure, who’s not, & who makes that choice.

•••

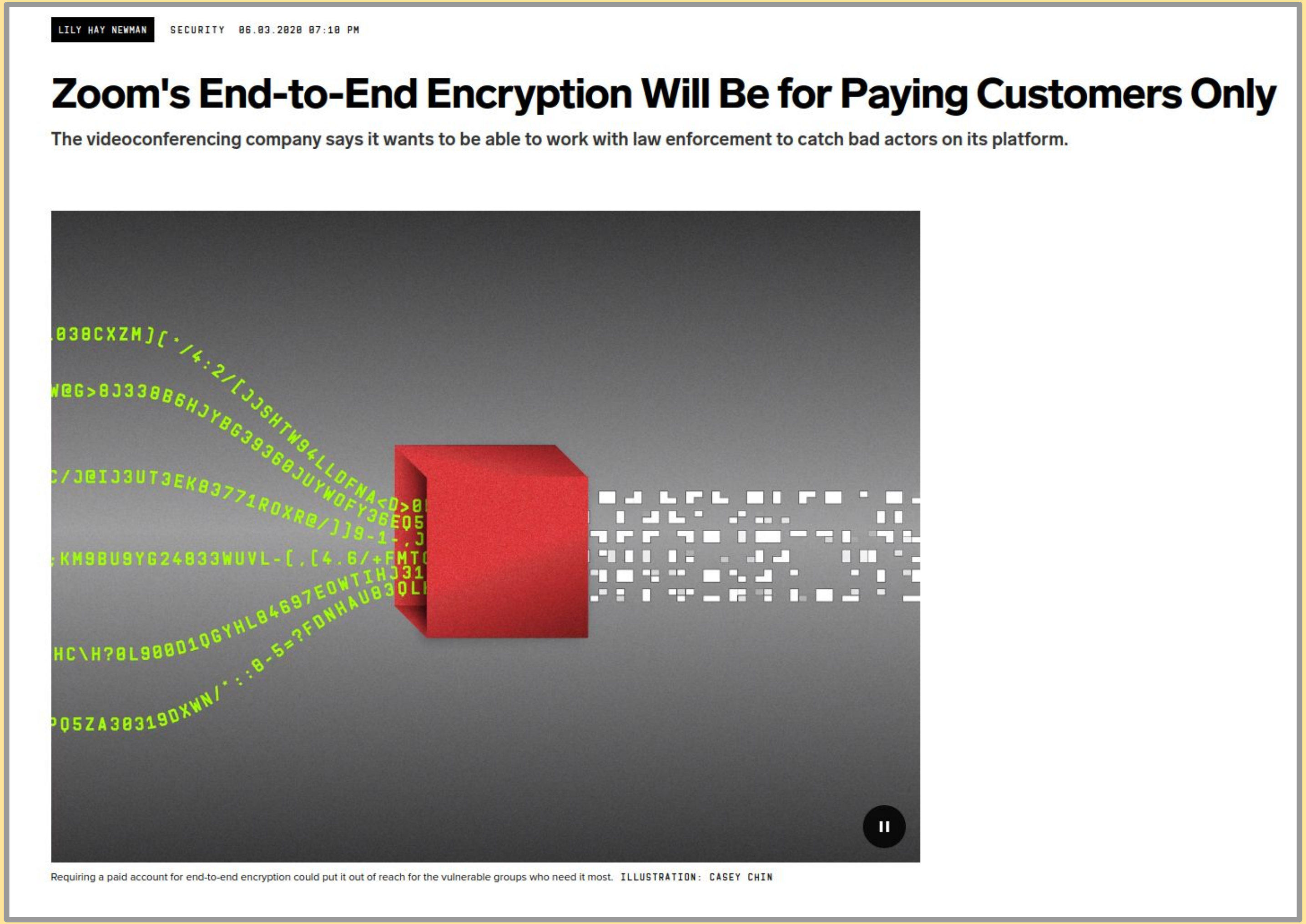
Who’s secure, who’s not, & who makes that choice.

•••

Spoiler: It’s us.

1) What is our role in the inequities in safe and secure access to technology?

2) What is our role in creating a more safe & secure society for all?



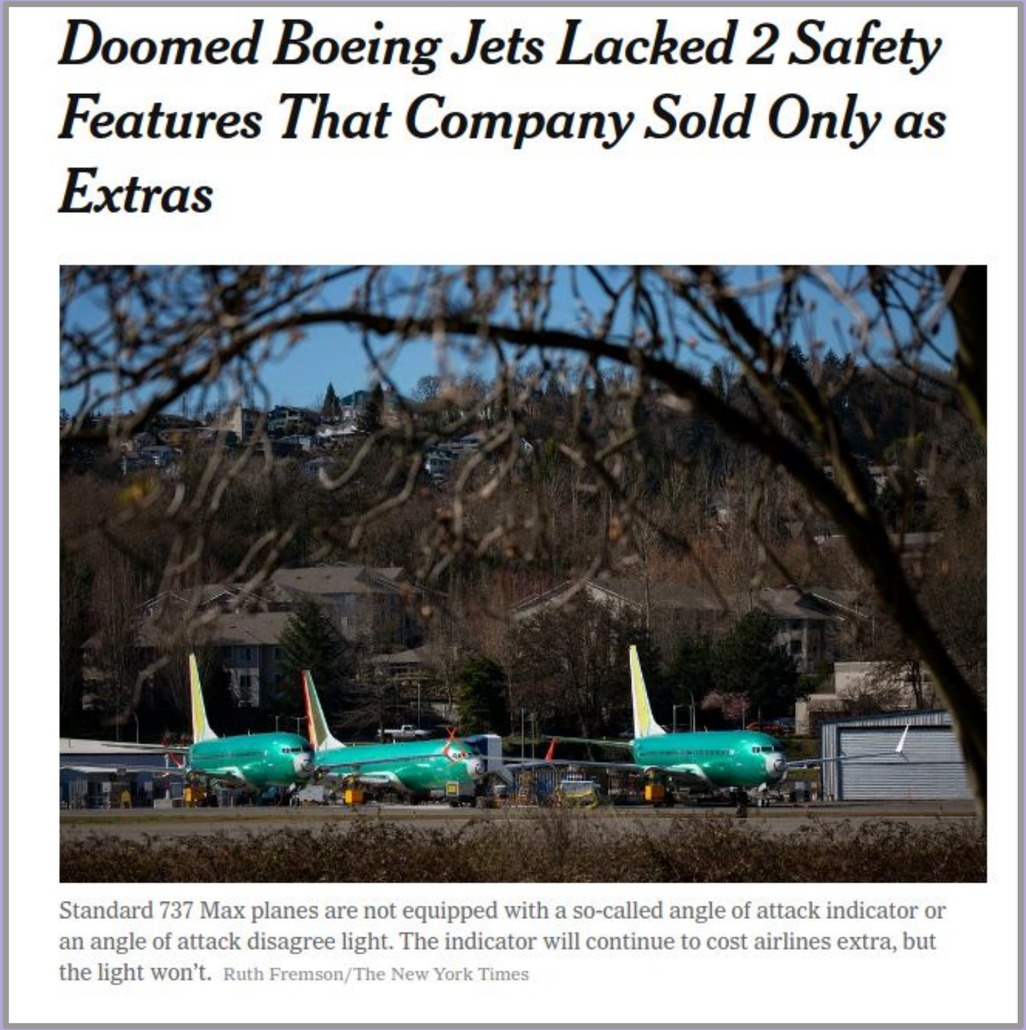
LILY HAY NEWMAN SECURITY 06.03.2020 07:10 PM

Zoom's End-to-End Encryption Will Be for Paying Customers Only

The videoconferencing company says it wants to be able to work with law enforcement to catch bad actors on its platform.

Requiring a paid account for end-to-end encryption could put it out of reach for the vulnerable groups who need it most. ILLUSTRATION: CASEY CHIN

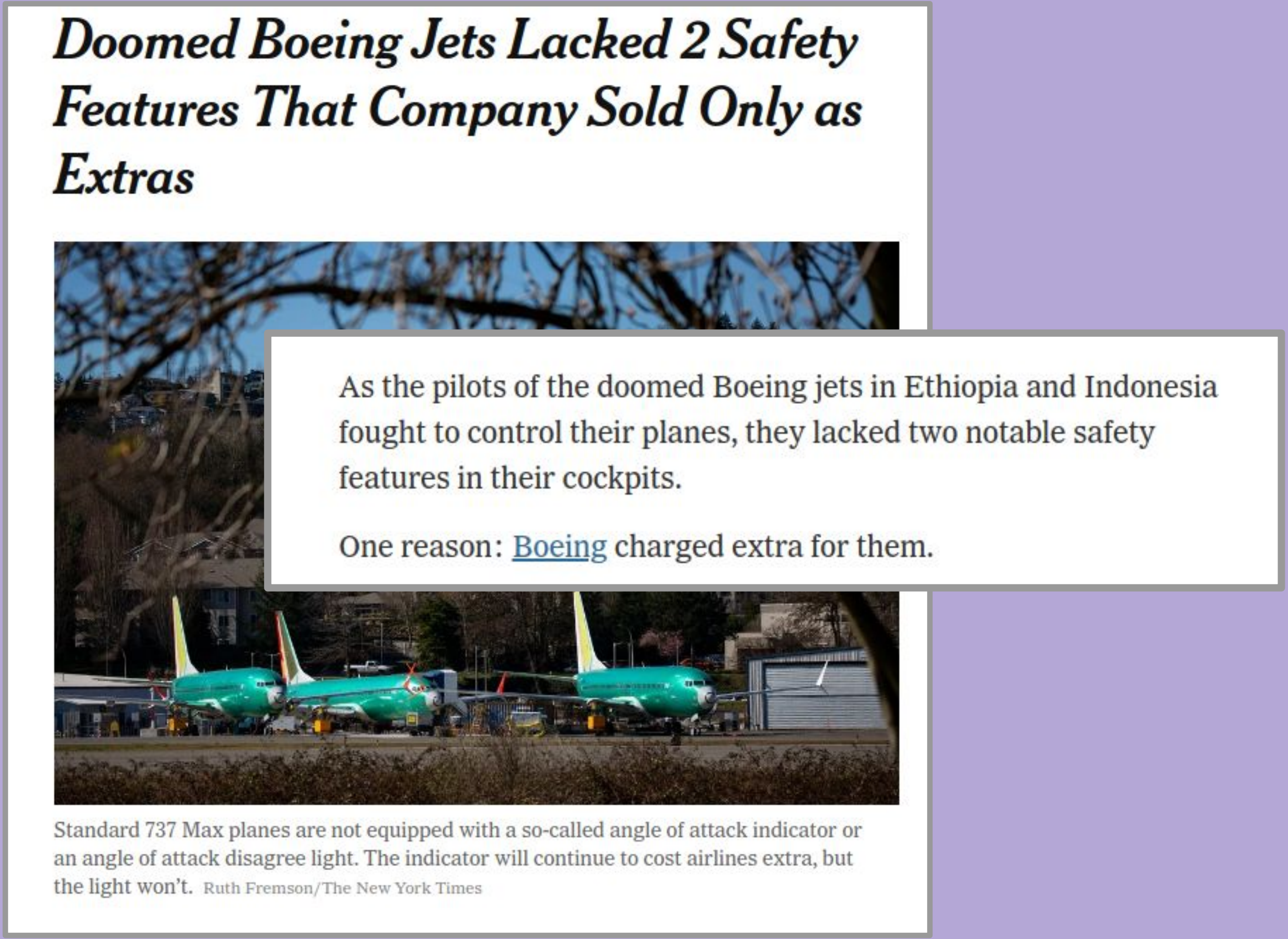
https://www.wired.com/story/zoom-end-to-end-encryption-paid-accounts/



Doomed Boeing Jets Lacked 2 Safety Features That Company Sold Only as Extras

Standard 737 Max planes are not equipped with a so-called angle of attack indicator or an angle of attack disagree light. The indicator will continue to cost airlines extra, but the light won't. Ruth Fremson/The New York Times

https://www.nytimes.com/2019/03/21/business/boeing-safety-features-charge.html



Doomed Boeing Jets Lacked 2 Safety Features That Company Sold Only as Extras

As the pilots of the doomed Boeing jets in Ethiopia and Indonesia fought to control their planes, they lacked two notable safety features in their cockpits.

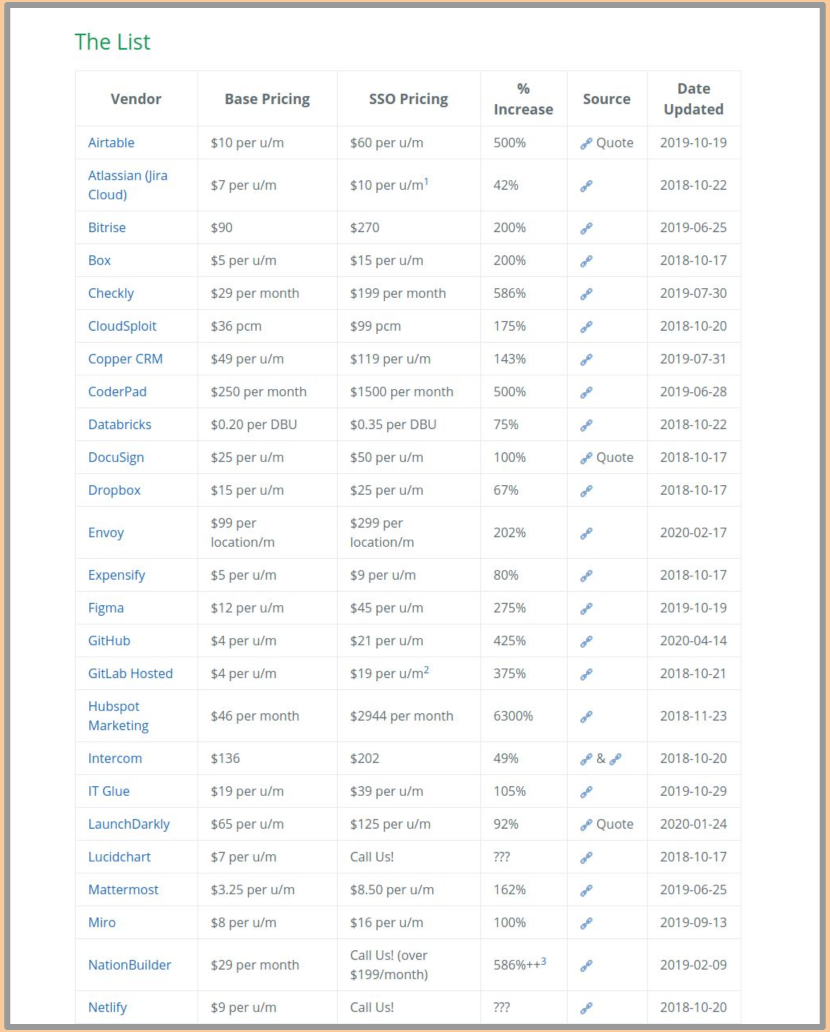
One reason: Boeing charged extra for them.

Standard 737 Max planes are not equipped with a so-called angle of attack indicator or an angle of attack disagree light. The indicator will continue to cost airlines extra, but the light won't. Ruth Fremson/The New York Times

https://www.nytimes.com/2019/03/21/business/boeing-safety-features-charge.html

Many SaaS companies charge 2-3x more for a customer to use single sign-on (SSO).

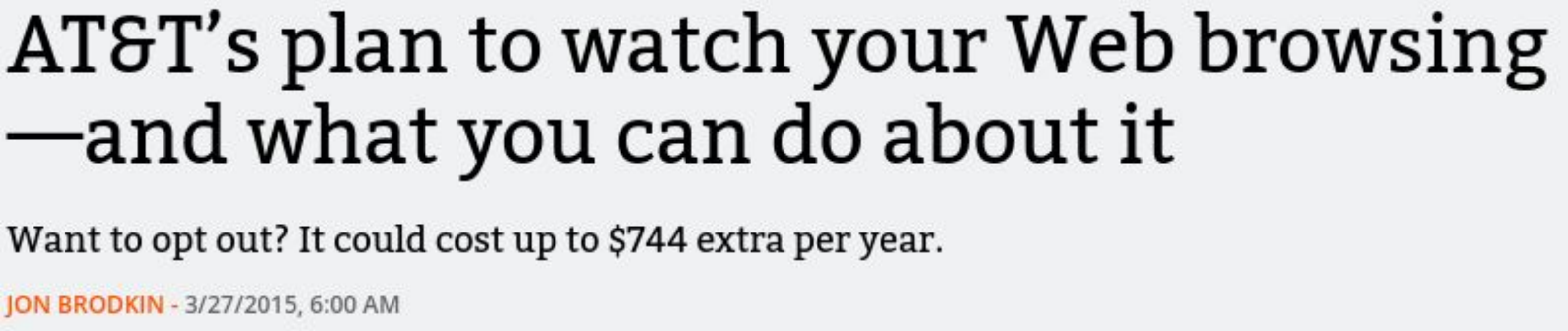
“SSO is a core security requirement for any company with more than 5 employees.”



The List

Vendor	Base Pricing	SSO Pricing	% Increase	Source	Date Updated
Airtable	$10 per u/m	$60 per u/m	500%	🔗 Quote	2019-10-19
Atlassian (Jira Cloud)	$7 per u/m	$10 per u/m[1]	42%	🔗	2018-10-22
Bitrise	$90	$270	200%	🔗	2019-06-25
Box	$5 per u/m	$15 per u/m	200%	🔗	2018-10-17
Checkly	$29 per month	$199 per month	586%	🔗	2019-07-30
CloudSploit	$36 pcm	$99 pcm	175%	🔗	2018-10-20
Copper CRM	$49 per u/m	$119 per u/m	143%	🔗	2019-07-31
CoderPad	$250 per month	$1500 per month	500%	🔗	2019-06-28
Databricks	$0.20 per DBU	$0.35 per DBU	75%	🔗	2018-10-22
DocuSign	$25 per u/m	$50 per u/m	100%	🔗 Quote	2018-10-17
Dropbox	$15 per u/m	$25 per u/m	67%	🔗	2018-10-17
Envoy	$99 per location/m	$299 per location/m	202%	🔗	2020-02-17
Expensify	$5 per u/m	$9 per u/m	80%	🔗	2018-10-17
Figma	$12 per u/m	$45 per u/m	275%	🔗	2019-10-19
GitHub	$4 per u/m	$21 per u/m	425%	🔗	2020-04-14
GitLab Hosted	$4 per u/m	$19 per u/m[2]	375%	🔗	2018-10-21
Hubspot Marketing	$46 per month	$2944 per month	6300%	🔗	2018-11-23
Intercom	$136	$202	49%	🔗 & 🔗	2018-10-20
IT Glue	$19 per u/m	$39 per u/m	105%	🔗	2019-10-29
LaunchDarkly	$65 per u/m	$125 per u/m	92%	🔗 Quote	2020-01-24
Lucidchart	$7 per u/m	Call Us!	???	🔗	2018-10-17
Mattermost	$3.25 per u/m	$8.50 per u/m	162%	🔗	2019-06-25
Miro	$8 per u/m	$16 per u/m	100%	🔗	2019-09-13
NationBuilder	$29 per month	Call Us! (over $199/month)	586%++[3]	🔗	2019-02-09
Netlify	$9 per u/m	Call Us!	???	🔗	2018-10-20

https://sso.tax/



AT&T’s plan to watch your Web browsing—and what you can do about it

Want to opt out? It could cost up to $744 extra per year.

JON BRODKIN - 3/27/2015, 6:00 AM

https://arstechnica.com/information-technology/2015/03/atts-plan-to-watch-your-web-browsing-and-what-you-can-do-about-it/

What do our actions say?

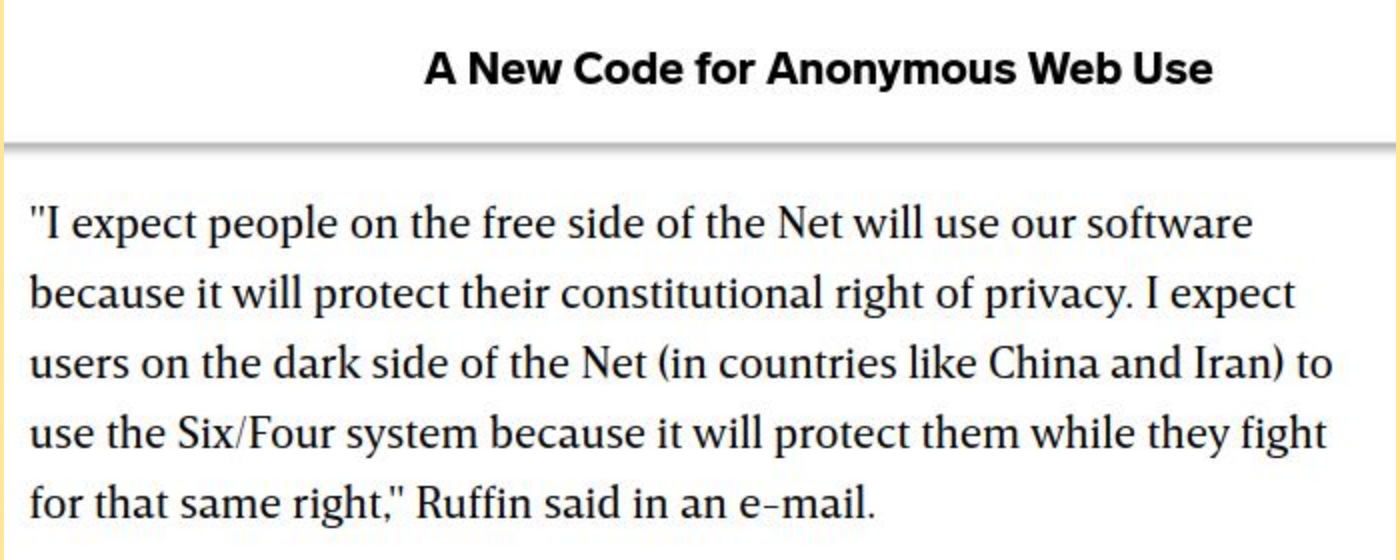
Security must be a requirement, not a feature.

Security must be a requirement, not a feature.

...Otherwise, we’re saying only the rich deserve to be secure.

Security, privacy, & safety are the minimal viable product.

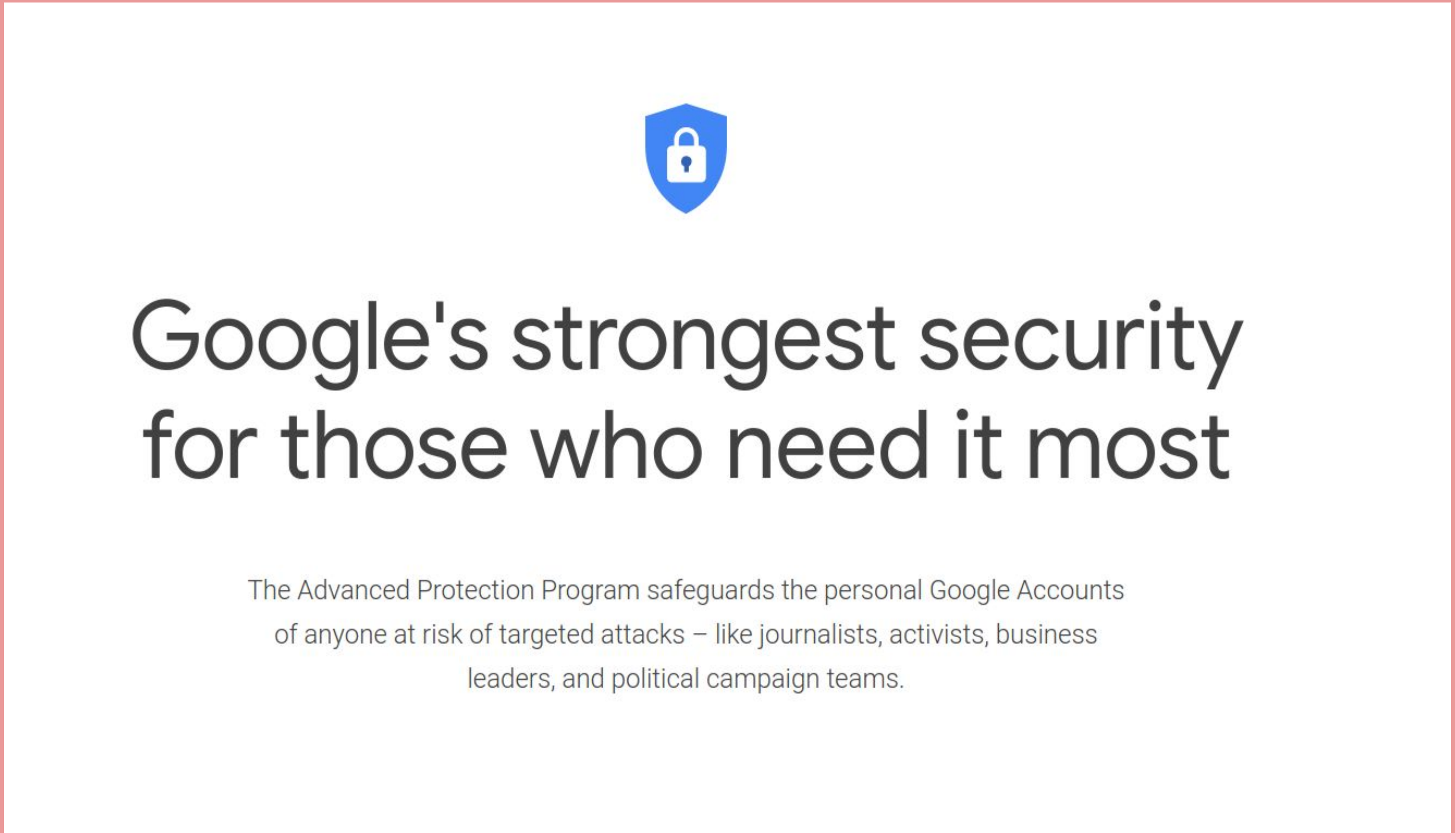
Infosec has always had a group of people that we’re trying to protect.



A New Code for Anonymous Web Use

"I expect people on the free side of the Net will use our software because it will protect their constitutional right of privacy. I expect users on the dark side of the Net (in countries like China and Iran) to use the Six/Four system because it will protect them while they fight for that same right," Ruffin said in an e-mail.

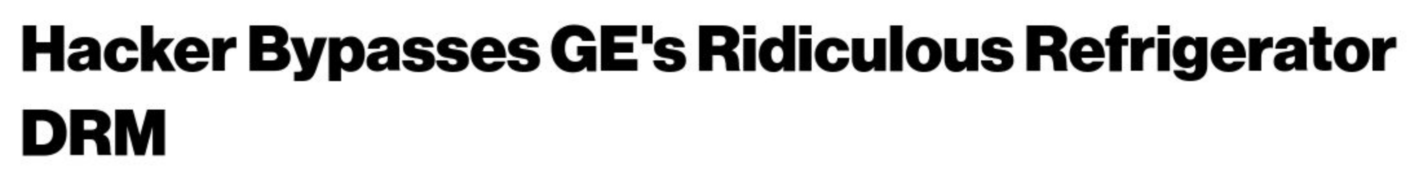
https://www.wired.com/2002/07/a-new-code-for-anonymous-web-use/



Google's strongest security for those who need it most

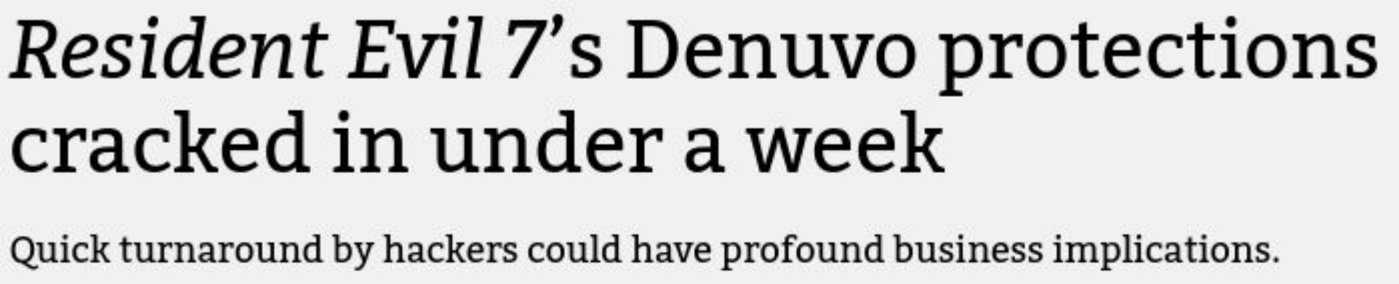
The Advanced Protection Program safeguards the personal Google Accounts of anyone at risk of targeted attacks – like journalists, activists, business leaders, and political campaign teams.

https://landing.google.com/advancedprotection/



Hacker Bypasses GE's Ridiculous Refrigerator DRM

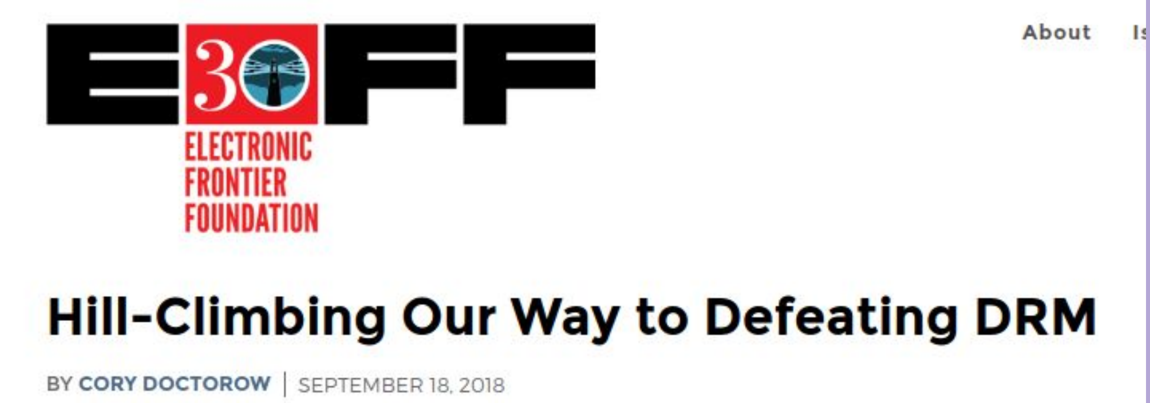
https://www.vice.com/en_us/article/jgxpjy/hacker-bypasses-ges-ridiculous-refrigerator-drm



Resident Evil 7's Denuvo protections cracked in under a week

Quick turnaround by hackers could have profound business implications.

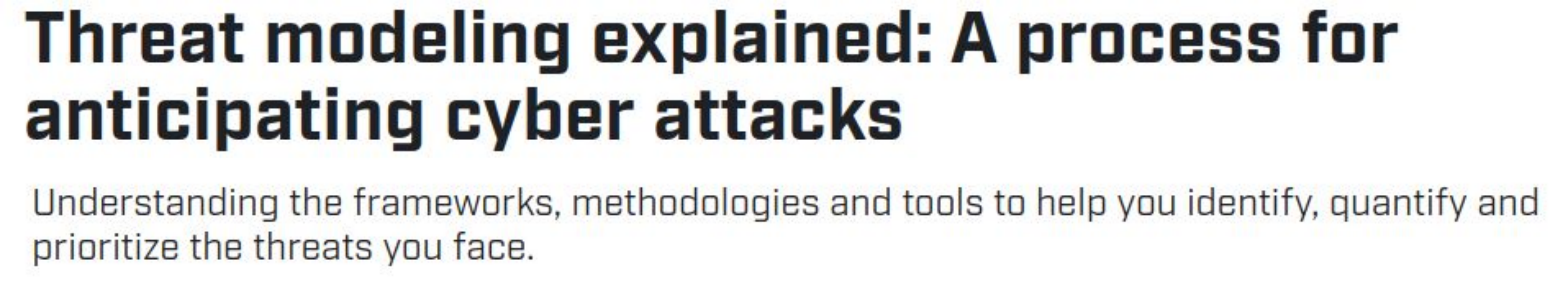
https://arstechnica.com/gaming/2017/01/resident-evil-7s-denuvo-protections-cracked-in-under-a-week/



Hill-Climbing Our Way to Defeating DRM

BY CORY DOCTOROW | SEPTEMBER 18, 2018

https://www.eff.org/deeplinks/2018/09/defeating-drm-hill-climbing-our-way-glory

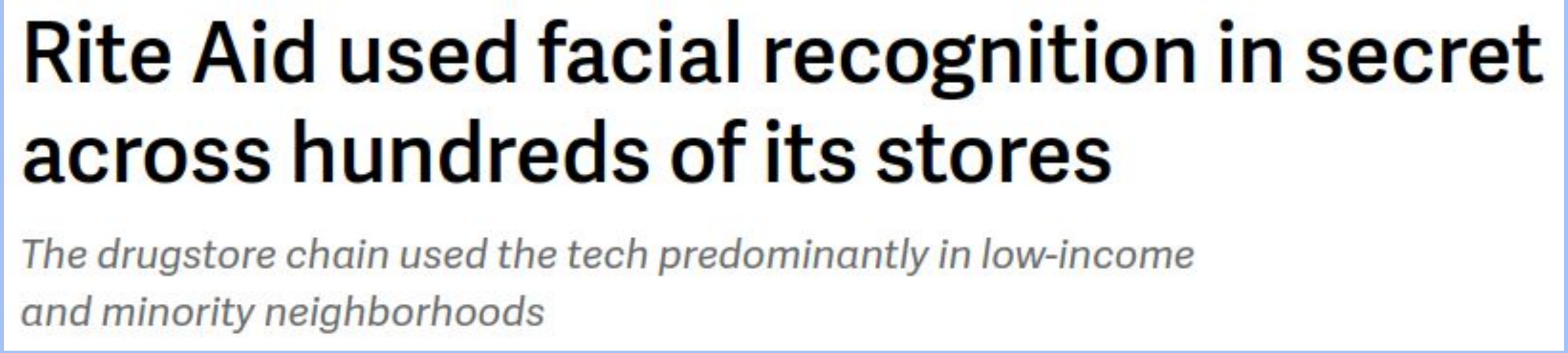


Threat modeling explained: A process for anticipating cyber attacks

Understanding the frameworks, methodologies and tools to help you identify, quantify and prioritize the threats you face.

https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html

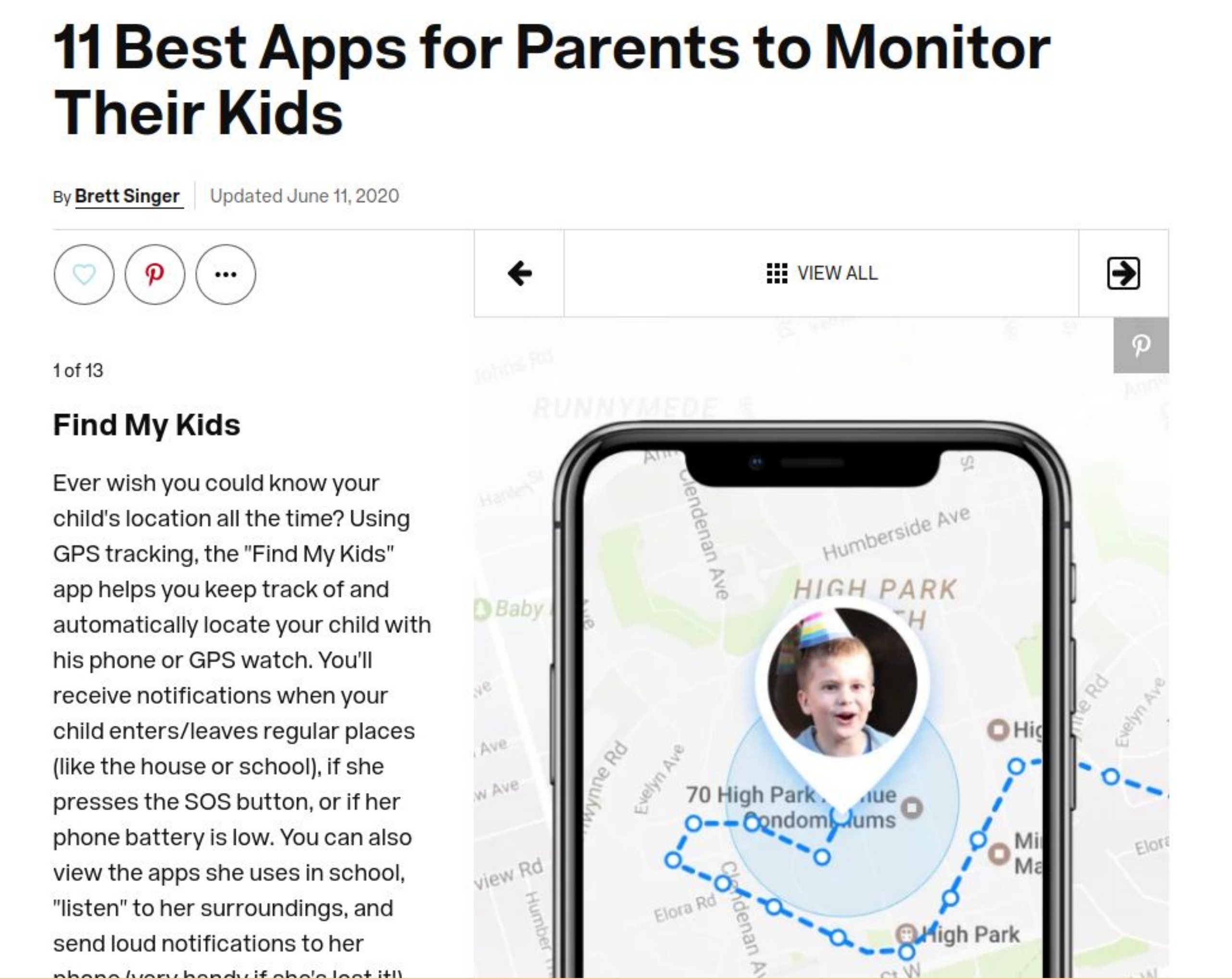
When we make a choice of who is protected, we also make a choice of who is not protected.



Rite Aid used facial recognition in secret across hundreds of its stores

The drugstore chain used the tech predominantly in low-income and minority neighborhoods

https://www.theverge.com/2020/7/28/21345185/rite-aid-facial-recognition-surveillance-spying



11 Best Apps for Parents to Monitor Their Kids

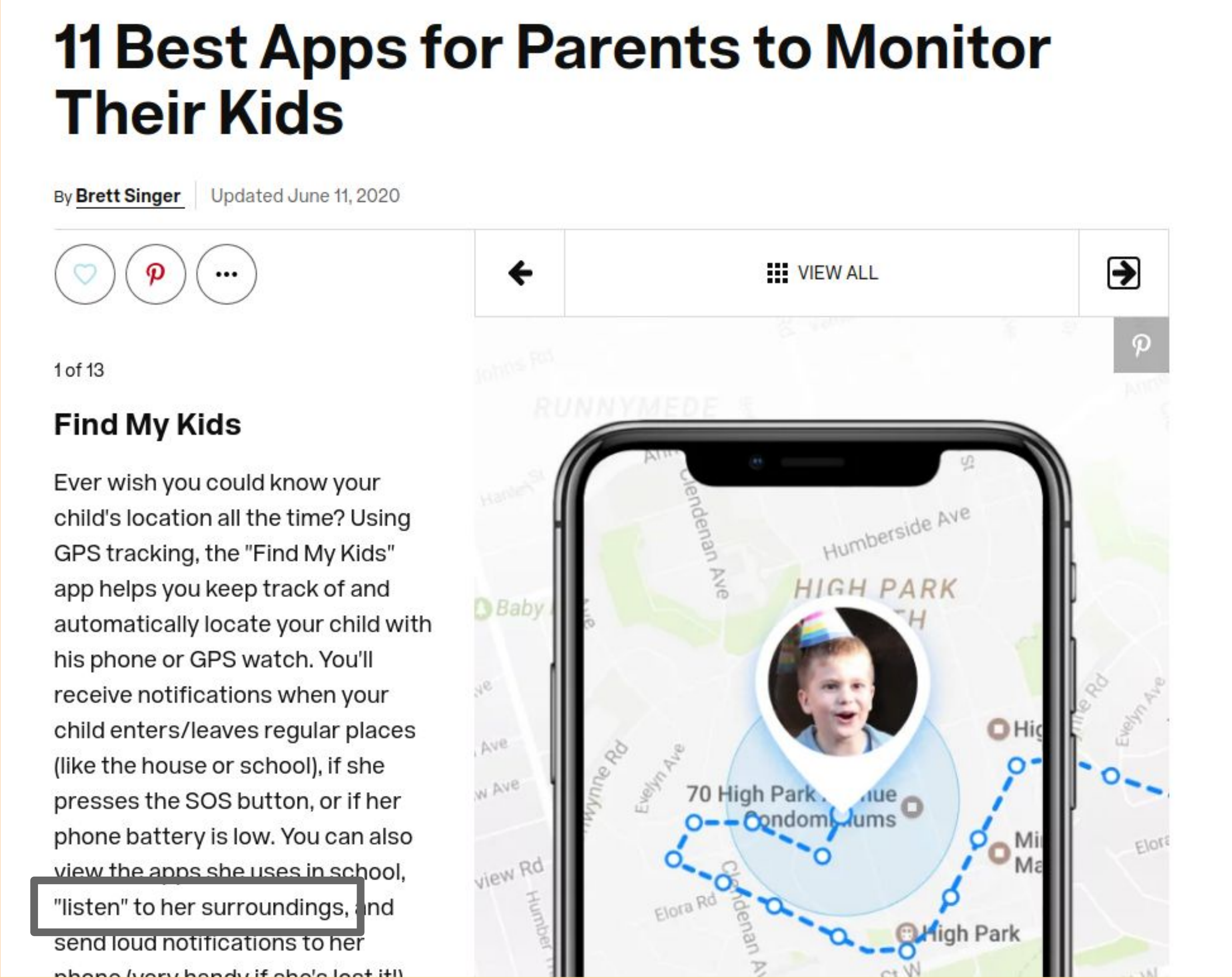
By **Brett Singer** | Updated June 11, 2020

1 of 13

Find My Kids

Ever wish you could know your child's location all the time? Using GPS tracking, the "Find My Kids" app helps you keep track of and automatically locate your child with his phone or GPS watch. You'll receive notifications when your child enters/leaves regular places (like the house or school), if she presses the SOS button, or if her phone battery is low. You can also view the apps she uses in school, "listen" to her surroundings, and send loud notifications to her phone (very handy if she's lost it!)

https://www.parents.com/parenting/technology/best-apps-for-paranoid-parents/



11 Best Apps for Parents to Monitor Their Kids

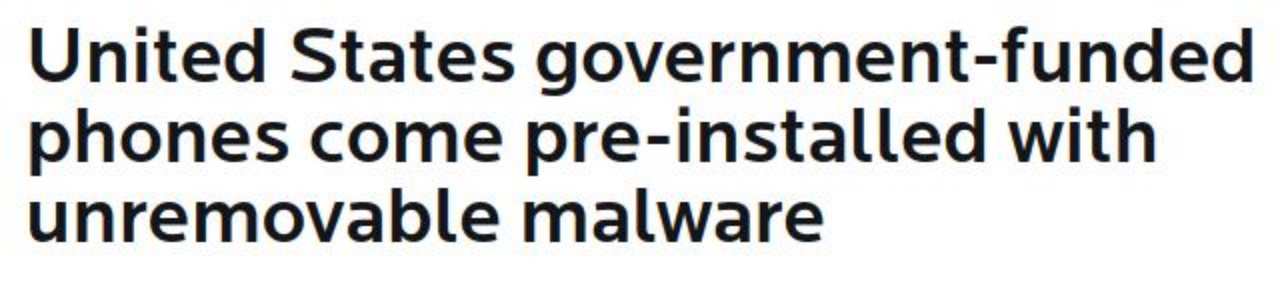
By **Brett Singer** | Updated June 11, 2020

1 of 13

Find My Kids

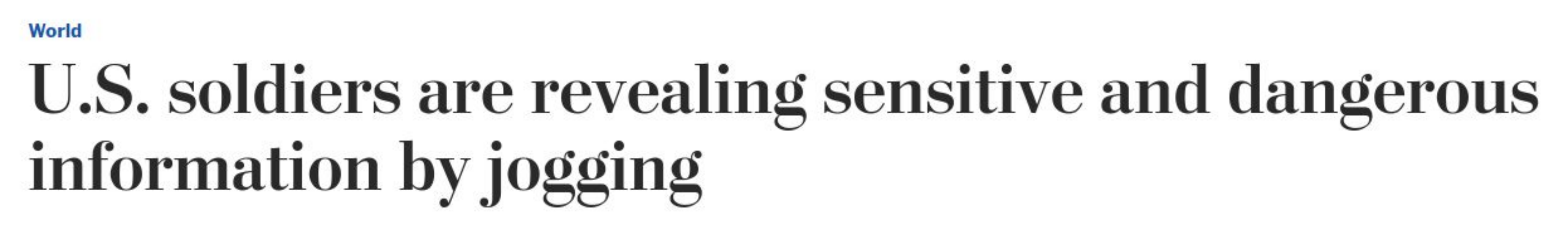
Ever wish you could know your child's location all the time? Using GPS tracking, the "Find My Kids" app helps you keep track of and automatically locate your child with his phone or GPS watch. You'll receive notifications when your child enters/leaves regular places (like the house or school), if she presses the SOS button, or if her phone battery is low. You can also view the apps she uses in school, "listen" to her surroundings, and send loud notifications to her phone (very handy if she's lost it!)

https://www.parents.com/parenting/technology/best-apps-for-paranoid-parents/



United States government-funded phones come pre-installed with unremovable malware

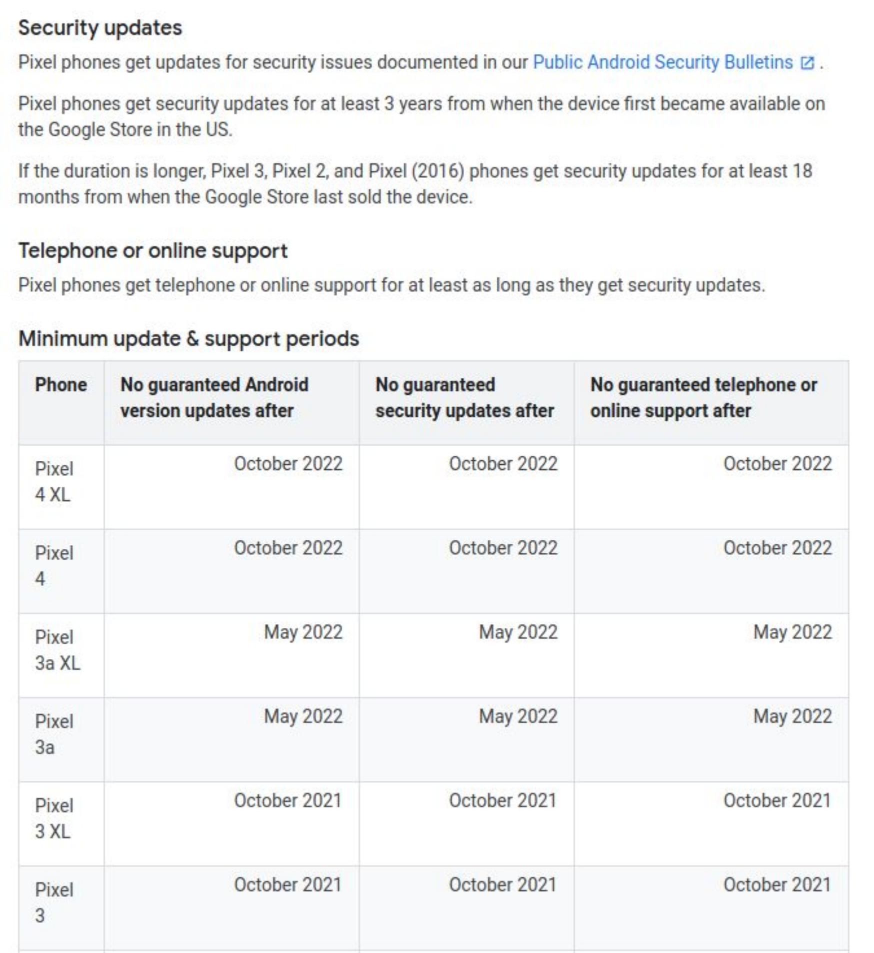
https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/



World

U.S. soldiers are revealing sensitive and dangerous information by jogging

https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html



Security updates

Pixel phones get updates for security issues documented in our Public Android Security Bulletins .

Pixel phones get security updates for at least 3 years from when the device first became available on the Google Store in the US.

If the duration is longer, Pixel 3, Pixel 2, and Pixel (2016) phones get security updates for at least 18 months from when the Google Store last sold the device.

Telephone or online support

Pixel phones get telephone or online support for at least as long as they get security updates.

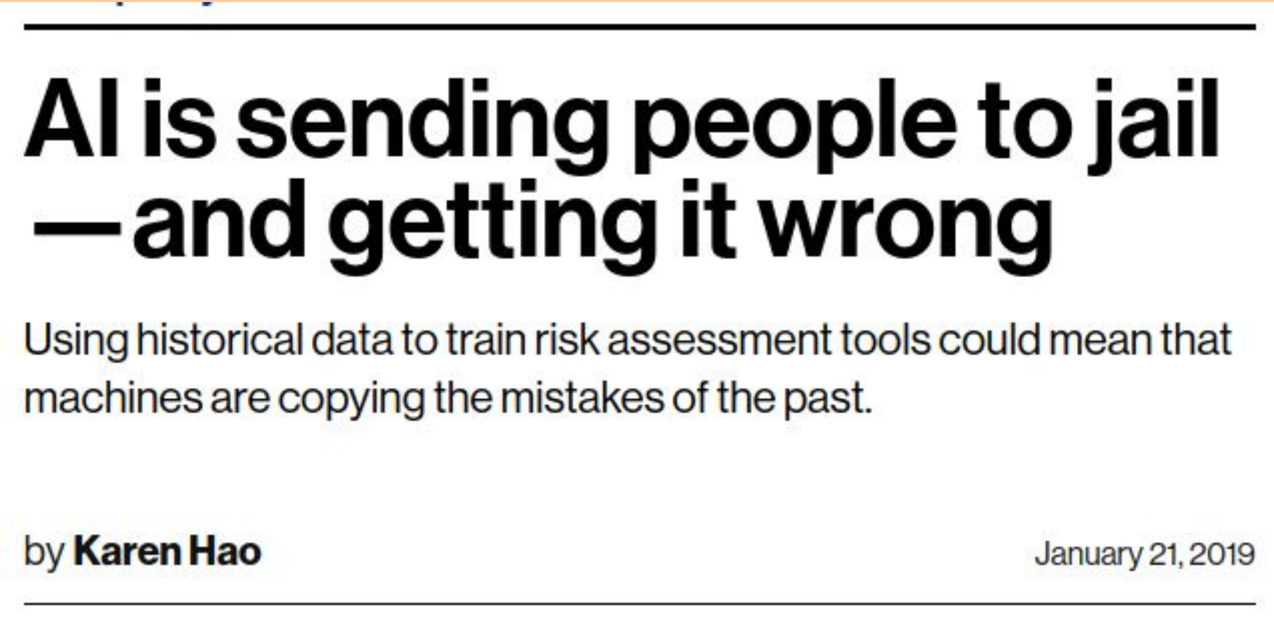
Minimum update & support periods

Phone	No guaranteed Android version updates after	No guaranteed security updates after	No guaranteed telephone or online support after
Pixel 4 XL	October 2022	October 2022	October 2022
Pixel 4	October 2022	October 2022	October 2022
Pixel 3a XL	May 2022	May 2022	May 2022
Pixel 3a	May 2022	May 2022	May 2022
Pixel 3 XL	October 2021	October 2021	October 2021
Pixel 3	October 2021	October 2021	October 2021

https://support.google.com/nexus/answer/4457705?hl=en

Each of our choices become patterns and the norm for how products are developed & released.

This then creates systemic inequalities in safety, security, & privacy.



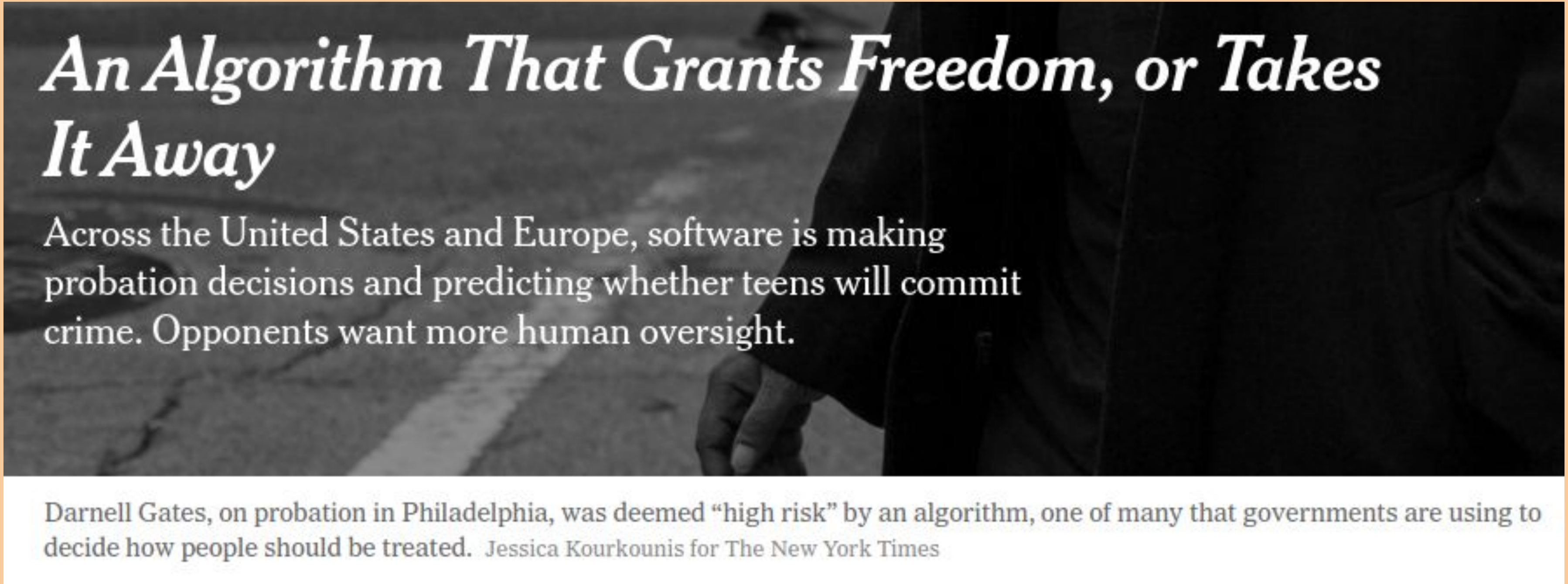
AI is sending people to jail —and getting it wrong

Using historical data to train risk assessment tools could mean that machines are copying the mistakes of the past.

by **Karen Hao**

January 21, 2019

https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/

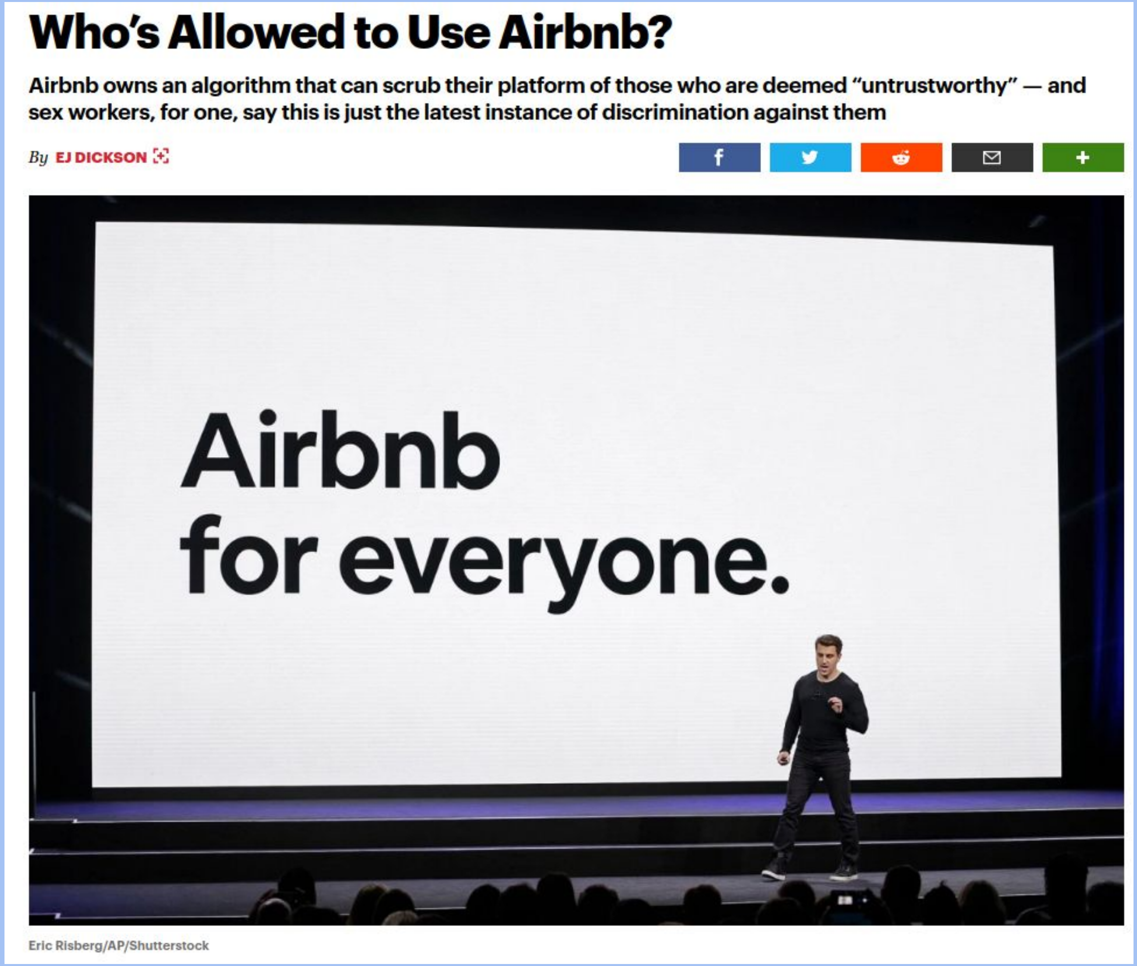


An Algorithm That Grants Freedom, or Takes It Away

Across the United States and Europe, software is making probation decisions and predicting whether teens will commit crime. Opponents want more human oversight.

Darnell Gates, on probation in Philadelphia, was deemed “high risk” by an algorithm, one of many that governments are using to decide how people should be treated. Jessica Kourkounis for The New York Times

https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html



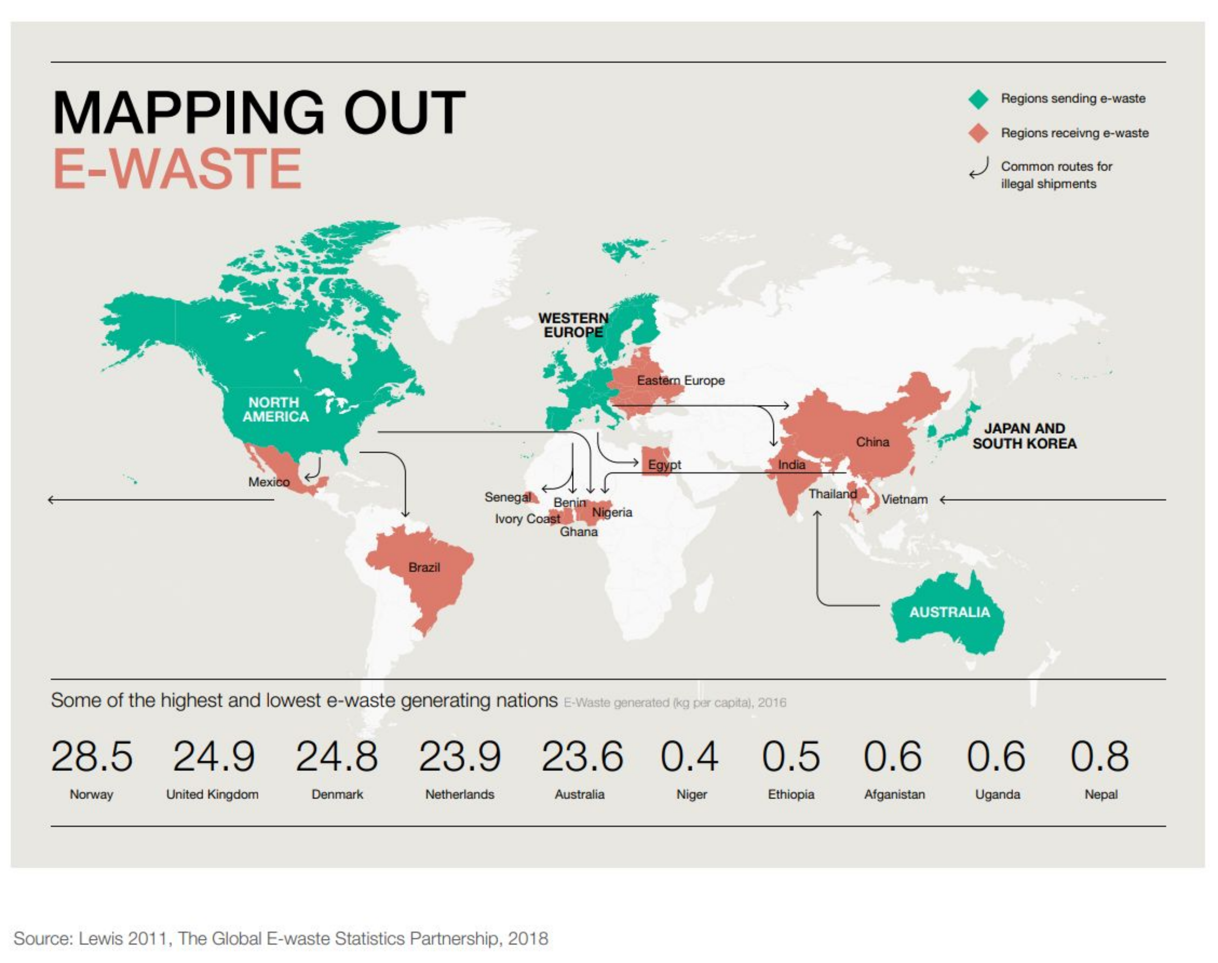
Who's Allowed to Use Airbnb?

Airbnb owns an algorithm that can scrub their platform of those who are deemed "untrustworthy" — and sex workers, for one, say this is just the latest instance of discrimination against them

By EJ DICKSON

Eric Risberg/AP/Shutterstock

https://www.rollingstone.com/culture/culture-news/airbnb-sex-worker-discrimination-935048/



MAPPING OUT E-WASTE

🟩 Regions sending e-waste

🟥 Regions receivng e-waste

↩ Common routes for illegal shipments

Some of the highest and lowest e-waste generating nations E-Waste generated (kg per capita), 2016

28.5	24.9	24.8	23.9	23.6	0.4	0.5	0.6	0.6	0.8
Norway	United Kingdom	Denmark	Netherlands	Australia	Niger	Ethiopia	Afganistan	Uganda	Nepal

Source: Lewis 2011, The Global E-waste Statistics Partnership, 2018

http://www3.weforum.org/docs/WEF_A_New_Circular_Vision_for_Electronics.pdf

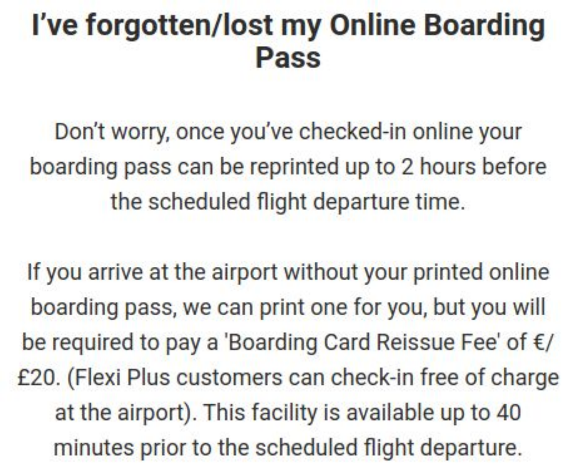
Mobile driver's license would replace the physical card with a digital identity

https://www.techrepublic.com/article/mobile-drivers-license-would-replace-the-physical-card-with-a-digital-identity/

Coronavirus Hastens the Rise of the Cashless Economy

Cashless transactions have spiked as company policies and consumer habits shift. But protections for people without bank and credit access haven't kept

https://www.bloomberg.com/news/articles/2020-07-14/the-costs-of-an-increasingly-cashless-economy



I've forgotten/lost my Online Boarding Pass

Don't worry, once you've checked-in online your boarding pass can be reprinted up to 2 hours before the scheduled flight departure time.

If you arrive at the airport without your printed online boarding pass, we can print one for you, but you will be required to pay a 'Boarding Card Reissue Fee' of €/£20. (Flexi Plus customers can check-in free of charge at the airport). This facility is available up to 40 minutes prior to the scheduled flight departure.

https://www.ryanair.com/hr/en/useful-info/check-in/boarding-cards

So what do we do?

1. Security is a requirement, not a feature.

2. Be explicit about who is helped and who is harmed.

3. Ensure your team represents the different experiences of your user base & those who are affected by your product.

WRITE

4. ~~Right~~ code and build products for the worst possible case that it could be used for.

Yes, this is hard.

If every one of us begins speaking up & taking actions, then that becomes the norm.

There is no neutral. So let’s use our power to help.

THANK YOU!

@maddiestone