Is Google's next product in the White House privacy report?

Summary: *OPINION: The 2014 White House Report on Big Data and Privacy was widely discussed, but one unmentioned section of the report reads like Google's five-year product projection.*

By Violet Blue for Zero Day | May 14, 2014 -- 12:16 GMT (05:16 PDT)

The 2014 *White House Report on Big Data and Privacy* includes a fictional vignette where a woman's life is made safer (and lives of those around her) because she's continuously monitored by external and internal surveillance products.

It's almost like reading Google's five-to-ten year product projection showcase.

The White House privacy report was published in multiple pieces (http://www.whitehouse.gov/issues/technology/big-data-review) on May 1, centralizing on two primary reports: Big Data and Privacy: A Technological Perspective (http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf) (Findings of the Big Data and Privacy Working Group Review) and Big Data: Seizing Opportunities, Preserving Values (http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf) .

The Big Data and Privacy Report was compiled by the President's Council of Advisors on Science and Technology (http://www.whitehouse.gov/administration/eop/ostp/pcast) (PCAST).

The privacy report made strong points about privacy risks, yet its weakened approaches to privacy protection and stance on allowing uncontrolled data collection to continue left some wondering (http://www.nytimes.com/2014/05/12/opinion/a-long-way-to-privacy-safeguards.html?_r=0) what interests will be served by the report's recommendations.

Google in particular has been singled out.

That's partly because PCAST includes Google's Eric Schmidt, but also because the report stresses that White House policy should leave data collection alone, stating that controlling collection isn't "scalable" and that enforcing collection control would be "economically damaging." And Google is conspicuously at the top of the collection business.

Another reason is because people like to blame Google for a lot regarding our seriously broken personal privacy these days. But it doesn't help that Google has more senior employees involved in the report than any other company.

Google's Eric Grosse and Peter Weinberger were among the "additional experts," and other companies making privacy policy recommendations to the White House include Booz Allen (http://www.zdnet.com/search?q=booz+allen) , Microsoft, In-Q-Tel (http://www.zdnet.com/search?q=%22In-Q-Tel%22) , Ernst & Young, Palantir, United Technologies Corporation and Zetta Venture Partners.

In this light, it's interesting to examine section 2.4 *Tradeoffs among privacy, security, and convenience* (pp 17-18).

Noting that it's important to consider that "notions of privacy change generationally" the report advises the White House that kids in the near future would be okay with things that might freak out anyone upset by "1984."

The report states, "Raised in a world with digital assistants who know everything about them, and (one may hope) with wise policies in force to govern use of the data, future generations may see little threat in scenarios that individuals today would find threatening, if not Orwellian."

PCAST conjures up an entire world in which surveillance products are a system of guardians, to protect us not only from threats of criminal intent or benign missteps such as missing one's plane -- but part of a futuristic system that protects us from the threat of deviation.

"PCAST s final scenario, perhaps at the outer limit of its ability to prognosticate, is constructed to illustrate this point."

The 2014 White House Privacy Report section reads:

Taylor Rodriguez prepares for a short business trip. She packed a bag the night before and put it outside the front door of her home for pickup. No worries that it will be stolen: The camera on the streetlight was watching it; and, in any case, almost every item in it has a tiny RFID tag. Any would-be thief would be tracked and arrested within minutes. Nor is there any need to give explicit instructions to the delivery company, because the cloud knows Taylor s itinerary and plans; the bag is picked up overnight and will be in Taylor s destination hotel room by the time of her arrival.

Taylor finishes breakfast and steps out the front door. Knowing the schedule, the cloud has provided a self- driving car, waiting at the curb. At the airport, Taylor walks directly to the gate no need to go through any security. Nor are there any formalities at the gate: A twenty-minute ―open door‟ interval is provided for passengers to stroll onto the plane and take their seats (which each sees individually highlighted in his or her wearable optical device).

There are no boarding passes and no organized lines. Why bother, when Taylor s identity (as for everyone else who enters the airport) has been tracked and is known absolutely? When her known information emanations (phone, RFID tags in clothes, facial recognition, gait, emotional state) are known to the cloud, vetted, and essentially unforgeable?

When, in the unlikely event that Taylor has become deranged and dangerous, many detectable signs would already have been tracked, detected, and acted on?

Indeed, everything that Taylor carries has been screened far more effectively than any rushed airport search today. Friendly cameras in every LED lighting fixture in Taylor s house have watched her dress and pack, as they do every day. Normally these data would be used only by Taylor s personal digital assistants, perhaps to offer reminders or fashion advice. As a condition of using the airport transit system, however, Taylor has authorized the use of the data for ensuring airport security and public safety.

Taylor s world seems creepy to us. Taylor has accepted a different balance among the public goods of convenience, privacy, and security than would most people today. Taylor acts in the unconscious belief (whether justified or not, depending on the nature and effectiveness of policies in force) that the cloud and its robotic servants are

Read this

EU digital chief attacks Do Not Track 'watering down'

Read more

trustworthy in matters of personal privacy.

In such a world, major improvements in the convenience and security of everyday life become possible.

The section ends there.

Next is "Collection, Analytics, and Supporting Infrastructure." The rest of the White House Privacy Report lacks fanciful short fiction pieces about productive citizens humans living in harmony with surveillance products connected to big data tracking and analytics.

The authors might say it's "Orwellian," but Mr. Orwell's near-satire of Stalinism was obvious.

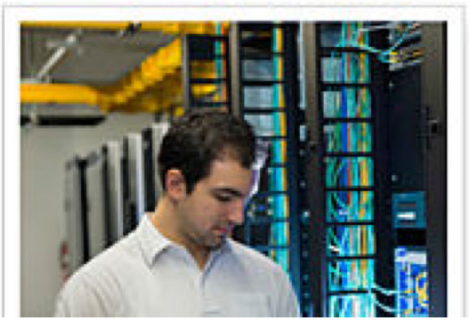
If it were a traditional product launch with so-called "first hint" and "conditioning" methodology, this kind of pitch would be way more subtle than Orwell. Even so, it's not hard to think of or imagine any number of Google projects, patents or acquisitions while reading the privacy report's little work of futurism.

I suppose we'll find out soon enough.

Topics: Security, Google, Government US, Privacy

About Violet Blue

Violet Blue is the author of The Smart Girl's Guide to Privacy. She contributes to ZDNet, CNET, CBS News and SF Appeal.



Top IT Certifications for 2014
(The Night Owl)

If You're Using Gmail, You Won't Believe This Trick
(Frank Addante)

Beacon Explainer– And why Apple's iBeacon is Ahead of the...
(Business Insider)

Talkback

What was left out was the terrorist

that positioned a one-shot remote gun pointed at the door for when the cameras picked her out exiting the door...

jessepollard
14 May, 2014 14:11

Reply *Vote*

C'mon It's Speculation

you didn't get the email re the script the house follows in cases like that? The house will, literally, pull the welcome mat out from under her causing the shot to miss. The house also knows where the remote terrorist is located (remember it's a remote controlled gun; the house has put a reverse trace on the IP signal on the gun when it was installed) and 1st responders are on their way to the terrorist's place

Crashin Chris
14 May, 2014 15:01

Reply *Vote*

Depends on the definition of "remote".

The house itself could have been hacked to pull the trigger...

jessepollard
14 May, 2014 19:43

Reply *Vote*

"In such a world,.....

...major improvements in the convenience and security of everyday life become possible."
Trust us.
Love,
Eric Schmidt and your Friends at Google

Userama

14 May, 2014 14:24

Reply *2 Votes*

Interesting that Eric Scmidt, a PCAST member basicly has it written that

Google should be left alone to do it's own thing...

William.Farrel

14 May, 2014 20:37

Reply *Vote*

Google - the new evil

http://marketmeat.wordpress.com/2014/03/13/is-google-the-new-evil/

anonymole@...

14 May, 2014 15:00

Reply *2 Votes*

With regard to 'deranged' and 'dangerous' ...

Quoted in the article:
"When, in the unlikely event that Taylor has become deranged and dangerous, many detectable signs would already have been tracked, detected, and acted on?"

One can quickly visit Merriam-Webster online and learn what these words mean, but what does the White House believe that they mean. For example, would attempting to wrest control of the government from corporations and returning control to the citizenry (exclusive of corporate citizens) be considered as 'deranged' and 'dangerous'?

And why the question mark at the end of the quote?

Rabid Howler Monkey

14 May, 2014 15:53

Reply *1 Vote*

You must be living on a different planet...

since, on planet Earth, and in today's world, especially in America, it's the government that has, virtually, seized control of corporations, and corporations are at the mercy of government goons, who have regulated businesses to the extent that, they're just extensions of government.

When American businesses have been trying to move operations and jobs out of the country, there is just one reason for that, and that is the intrusiveness that government has brought to everyday lives and everyday business.

adornoe@...
15 May, 2014 16:09

Reply *Vote*

Govt. & Corporate Entities...

...are one.

BTW, where'd the mob go?

USDK
17 May, 2014 14:36

Reply *Vote*

Propaganda

So, the White House privacy report basically is just trying to convince everyone to give up all semblance of privacy. Did I hear someone say "propaganda"?

AnomalyTea
14 May, 2014 15:57

Reply *1 Vote*

It's not about privacy, nor about propaganda...

it's about how government, with the willing and controlled businesses, have an agenda to control the people and all of their movements and their whole lifestyles.

The agenda is to control. And there are way too many that feel that, they're better off with government control of their lives

control of their lives.

adornoe@...

15 May, 2014 16:12

Reply *Vote*

Why Female Fictional Vignette?

This could be applied to any person who doesn't feel safe and believes such capabilities would mitigate those feelings. Does it not sound as believable when the fictional character is a 300lb, 6'6", beef-cake Pro Football player?

OK -- I digress.

"When her known information emanations (phone, RFID tags in clothes, facial recognition, gait, emotional state) are known to the cloud, vetted, and essentially unforgeable?"

Really? The movie "Gattaca" gives us a glimpse of a similar world based on DNA identification. Granted, this is Hollywood but how they fool the "system" seems plausible. If a DNA-based system can be fooled, who believes we can create unforgeable electronic credentials?"

robradina@...

14 May, 2014 18:45

Reply *1 Vote*

Forget Gattaca and Hollywood

We get a pretty good glimpse at how every supposedly secure system ever created has been hacked and breached. They have already spoofed and forged current RFID tag technology. Techno-terrorists can easily and seriously disrupt any of these highly sophisticated systems using rather unsophisticated EMP causing plenty of inconvenience and potentially billions of dollars.

Anyone who would willingly trade their privacy and personal security for the false sense of security provided by people who control both the tech and how it is used would be a fool.

techadmin.cc@...

15 May, 2014 06:23

Reply *Vote*

When does deviation become deviance?

I suspect most adult human beings currently not living in a convent, would find the idea of being constantly monitored by friendly cameras something more than a trade-off of privacy for security. Most of us probably occasionally do things in private that we would not want exposed, recorded, or evaluated by uninvited behavioral specialists or their cybernetic personal assistants. Unless the society of the future becomes so tolerant that nothing short of viciously violent attacks against a person would raise a robot eyebrow, populated by either perfectly behaved or shameless cretins proud to expose their every thought and action...Oh wait...Facebook.

geonque

14 May, 2014 18:49

Reply *1 Vote*

WOW

The possibilities for abuse of such a system and the people that are part of it boggle the mind. If only the corporate/political agenda was in the best interests of all of the people of the world.

rickscr

14 May, 2014 19:55

Reply *Vote*

Join the Google crusade! (for unrestricted personal information gathering)

Use Android, Chrome, and Google apps!
/s

Userama

14 May, 2014 20:13

Reply *2 Votes*

And yet aren't people today feeling indignation towards the NSA

for doing something far less intrusive? But those same people will happily live in the world described above?

Do the PCAST members watch the news, or was the committee created to give Google a free pass on everything?

William.Farrel

14 May, 2014 20:43

Reply *1 Vote*

Before Google or any company, or any government entity, gets to the point

of tracking each and every more we make, the government and those businesses will have had to undo a few of the amendments to the constitution, if not all of them. Heck, the constitution itself would have had to be repealed.

Think about one of those amendments alone: the 4th.

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

That government or any entity acting on behalf of that government, would have access to a person's every move and every action and every statement uttered, and every conversation, could open up any person to prosecution, for any reason that a government entity deems anti-government or illegal, or treasonous, or dangerous to other people or themselves.

We have already witnessed that kind of government activity with the IRS scandal, where certain government operatives decided to target those who disagreed with their politics; namely, the targets were conservative groups and "tea party" supporters.

So, what is to stop the government from becoming totalitarian when they control the means to monitor each step of our lives?

adornoe@...

15 May, 2014 16:27

Reply *Vote*