SB 5062 – Bad Washington Privacy Act

Commentary by Jon Pincus, jon@achangeiscoming.net

Original version: March 24, 2021

Last updated: April 4

An unsigned and unattributed document, titled a "quick summary", is an excellent illustration of the techniques supporters of the spin techniques Bad Washington Privacy Act are using.

Comments in bold are from me; I've also highlighted the disinformation techniques the bill's supporters are using here — misleading framings, statements, and omissions; inaccuracies; and the kernel of truth that good disinformation often leverages or obscures. Keep these techniques in mind as you read other pro-BadWPA talking points and material.

I'll go through the first few in detail; after that, I'll be briefer. At the end I go into more detail on opt-in/opt-out.

The document, and the original version of this analysis, referred to the Senate version of the bill. Sections marked UPDATE ***discuss changes since then, including CR&J striker.***

MISLEADING FRAMING: The Bad Washington Privacy Act, if passed, will be the strongest consumer data privacy in the nation.

So what?

What matters to your constituents — and your friends and families — is whether or not the bill you pass protects them. Isn't that what we should be talking about?

Civil rights immigrant rights, and civil liberties organizations, and independent experts, have repeatedly said it doesn't. So have consumer and privacy groups -- even ones who endorse it point out areas where it falls short. Once they hear what's in the bill, most Washingtonians don't think it protects them.

Of course lobbyists who benefit from an ineffective bill that lets them keep exploiting your constituents assure you that it does protect consumers. Your task as legislators is to decide who to believe.

But whoever wrote this document doesn't want to discuss that. Instead, they're trying to use the extremely low bar set by other bills as a standard so that their claims of "the strongest privacy law in the US" make it sound good.

They're also trying to shift the discussion to whether it's slightly better than other bad bills. They reinforce this later in the doc by lengthy comparisons below, which make it seem this is an important topic you should be paying a lot of attention to. And the

Just because an Amazon lobbyist gave a privacy bill Washington had rejected to the Virginia legislature and they whisked it through doesn't mean it got better in the process. It might have even gotten worse.

MISLEADING OMISSION: **People aren't just consumers. They might also be students or employees or others that are explicitly excluded.**

KERNEL OF TRUTH, OBSCURED**: Other states also have unenforceable bills with loopholes and definitional problems that neuter the protections the bill claims to provide. Tech lobbyists and their partners like data brokers and the ad industry are influential in other states as well as here. The approaches of giving out lavish exemptions to get broad backing, and using stealthy language to make a bad bill look stronger than it is, work everywhere (and not just for privacy).**

MISLEADING: This is the third session the legislature has considered a version of this bill. Over the last three years, stakeholders have had the opportunity to add stronger consumer protections.

"The legislature" hides the difference between the chambers.

The House has indeed given stakeholders the opportunity to add strong consumer protections.

The Senate has not, and the bill's primary sponsor has been very open about it. For example, In his Seattle times op-ed, he said that only those "on the rigid edges of political ideology" oppose his bill.

KERNEL OF TRUTH, OBSCURED**: Tech companies have also had plenty of opportunities to add strong consumer protections to the bill. They haven't done that.**

UPDATE**: The CR&J striker provides a good example of stakeholders adding stronger protections. Consumer Reports and Common Sense got a global privacy control (better opt-out, but it's still opt-out), opt-in for minors (another recognition**

that opt-in provides better protection, although still only applying it in a very limited way), a very limited PRA that they both have said should be stronger, and a one-year sunset on the right to cure. Also, non-profits now have a permanent exemption; that's a strong protection for Consumer Reports and Common Sense, not consumers. So now they both support the bill despite clearly thinking it should be stronger -- Consumer Reports for example describes the right to cure as a "get-out-of-jail-free" card" that "signals that a company won't be punished for breaking the law".

INACCURATE: The version before you now represents significant input from Consumer groups, the House and from the State's Attorney General's office in previous sessions.

Significant input has been provided — but is not represented in this version.

Look at last year's op-ed by authors from consumer groups Consumer Federation of America and WashPIRG, this year's op-ed by an author from Consumer Reports, or the more detailed comments these groups have submitted. Significant input. Not represented.

Last year's House improvements? Significant input. Almost none of it is represented.

The AGO fares only a bit better: per se is represented (that's also the only House input represented as far as I know). But the AGO's significant input on private right of action, "broad exceptions that would permit industry to sidestep the very consumer rights and obligations created by this bill" and limit their enforcement ability, and the right to cure … is not represented.

KERNEL OF TRUTH, OBSCURED: Some stakeholder input is indeed represented. One small recent example: the Senate amended the bill to exempt the airline industry. And since Microsoft liked last year's bill so much they proposed it as a model for the nation, an Amazon lobbyist lobbyist gave it to a Virginia legislator to use as the basis for their law, and Google supported it this year, their input is probably represented quite well.

MISLEADING OMISSION: What about privacy, immigrant rights, civil rights, civil liberties, and grassroots activism groups who aren't even mentioned here? They too have provided significant input that's not represented here. As several Tech Equity Coalition groups said in a letter to the bill's primary sponsor about his September draft

The current draft largely follows the approach of the unsuccessful Senate version of SB 6281, which we and many others strongly opposed earlier this year. Organizations including Japanese American Citizens League -- Seattle Chapter, One America, InterIm CDA, Black Lives Matter Seattle King County, Washington Association of Criminal Defense Lawyers, CAIR Washington, Densho, the John T Williams Organizing Committee, La Resistencia, MAPS AMEN, Real Change, Urban League of Metropolitan Seattle, Consumer Federation of America, Privacy Rights Clearinghouse, EPIC Privacy, EFF, and ACLU of Washington invested a lot of time and energy identifying problems on SB 6281 -- and suggesting improvements.

The draft would benefit from including the feedback from their open letters, official comments, and testimony.

That input was also ignored. There wasn't even a response to the comments.

1. **What does the bill do?**
   a. MISLEADING: Provides consumers the following rights. **But these "rights" are not enforceable, and limited in various ways**
      i. Visibility re: their personal data
      ii. Access to their personal data
      iii. MISLEADING: Option to delete their data:
      See Jennifer Lee's testimony at the hearing.
      UPDATE**: there were significant improvements in the CR&J striker - but that just highlights how misleading the statement was before.**
      iv. Ability to move data to another platform
      v. MISLEADING**:** Option to correct data:
      Same issues as the right to delete.
      vi. MISLEADING: Ability to opt-out of sales of their data, targeted advertising and/or consequential profiling:

      Opt-out rights are limited in many ways, for example no opt-out of Facebook's targeted advertising based on browsing behavior on their site, no opt-out of sales of data to affiliate

      MISLEADING OMISSION: **WPA does not allow opt-out of sales of data to affiliates, or use of data "based on activities within a controller's own websites**

or online applications" for targeted advertising. So Google can use your behavior on their web site and apps for targeted advertising, and

vii. MISLEADING: Opt-in consent for sensitive data including location data. **"Sensitive data" clause can be inferred with high probability from non-sensitive data that is only opt-out, so this supposed right is illusory**

viii. MISLEADING OMISSION: **WPA does not protect student data, employment data, financial data subject to GLB, etc**.

b. MISLEADING: Requires companies to be good stewards of collected data:

Without effective enforcement, requirements are not real

i. Minimize the data collected to disclosed purposes only

ii. Limits use of data to disclosed purposes only

iii. Requires implementation of data security safeguards

iv. INACCURATE: Prohibits companies from processing data to discriminate.

As Brianna Auffray testified at the way the language is worded, it would be very difficult to charge anybody with violating it

2. Who is subject to the bill?

a. Businesses with 100,000 transactions or more; or

b. Businesses that derive more than 25% of their revenue from data sales

c. INACCURATE: Non profits::
Section 403 exempts non-profits for four years
UPDATE**: non-profits are now permanently exempt**

d. Government is not included.

e. Higher education is delayed for five years

f. MISLEADING OMISSION: **airlines are not included**

3. How is the bill enforced?

a. AG enforcement under the Consumer Protection Act.

b. **MISLEADING**: AG is granted all presumptions for ease of enforcement

AGO testified last year that the bill's broad exceptions "would permit industry to sidestep the very consumer rights and obligations created by this bill" limited their enforcement ability, and the exceptions in the year's bill are even broader. And, AGO has testified that the "right to cure" will cause a drain on their resources.

c. **MISLEADING:** AG has testified the bill is enforceable.
AG has testified that the bill should have private right of action.

KERNEL OF TRUTH, OBSCURED: Last year's bill was not enforceable. Sponsors and supporters claimed that it was. They lied.

d. **MISLEADING OMISSION**: Companies are allowed 30 days to rectify an error (right to cure) once notitfied.
AGO has testified that the "right to cure" will cause a drain on their resources.
Consumer Reports describes the right to cure as a "get-out-of-jail-free" card" that "signals that a company won't be punished for breaking the law".

e. **MISLEADING OMISSION**: No private right of action.
AG has testified that a private right of action is necessary to protect Washingtonians
UPDATE: there is now a very limited private right of action, allowing injunctive relief, attorney's fees, and costs

f. **MISLEADING OMISSION**: **the fiscal note only allocates enough money for 3.6 AG FTEs. This is only enough to bring three cases per year, so not an effective deterrent. By contrast, Ireland — the same size as Washington — budgets 20x as much for enforcement.**

4. **MISLEADING**. The Bad WPA provides stronger consumer protections than California's CCPA.
California's CCPA has not resulted in any significant enforcement actions so far — and it is being replaced by the CRPA. So it is a failure, a very low bar for comparison. In any case, the question isn't whether Bad WPA is stronger than other weak laws, the question is whether it protects Washington consumers. So really we could stop here. But it's still interesting to look at the specific claims under this bullet.

    a. **MISLEADING**: Bad WPA Requires opt-in consent for sensitive data; California is opt-out for sensitive data.
    Most if not all of the other categories included in the Bad WPA's "sensitive data" clause can be inferred with high probability from non-sensitive data that is only opt-out, so this supposed protection does not have the impact it appears to. For example, race is sensitive; what color makeup you wear is not but in many cases implies your race. Combine this with other non-sensitive data and companies can identify information with high likelihood.

b. MISLEADING: Bad WPA Allows consumers to opt-out of consequential profiling; California does not have this provision.
Opt-out is not effective protection in general; and, in this case there is no way for the customer to know the profiling is happen so opt-out is effectively useless

c. MISLEADING: Bad WPA opt out for targeted advertising is broader; California opt-out only applies to transfer of data for targeted advertising.
Opt-out is not effective protection in general; and WPA opt-out for targeted advertising has significant limitations

d. MISLEADING: Bad WPA Right to delete is broader; California only applies to data collected from a consumer, not data collected from other companies.
WPA's right to delete is insufficient to protect victims of crime like stalking, harassment, and domestic violence. It doesn't matter whether California's is worse.

e. MISLEADING: California does not cover data brokers - Bad WPA does.
Bad WPA's broad exceptions significantly limit its effectiveness covering data brokers.

f. MISLEADING: WPA addresses civil rights; California does not.:
Every civil rights organization that has testified on this or earlier versions of the WPA has opposed it. It's true that California's doesn't even pretend to address civil rights but that doesn't mean that the Bad WPA's language purporting to address this is acceptable.

5. How does enforcement differ between CCPA and WPA?

    a. MISLEADING OMISSION: Both bills use AG enforcement for data privacy provisions.
    CCPA's lack of a right of private action means there have been few enforcement actions. So this similarity is actually strong argument against Bad WPA..

    b. California's bill includes a private right of action for data breach

    c. Washington already has separate statute covering data breach (RCW 19.255), including a private right of action

    d. MISLEADING OMISSION**: Both bills have a "right to cure". CCPA's right to cure was a failure. It was removed in the CRPA.**

6. Why doesn't the bill require opt-in for all data collection and processing?

INACCURATE; MISLEADING: In the WPA, consumers are provided rights so they can affirmatively choose how their data is managed.

Many of the "rights" inBad WPA are opt-out, which is not "affirmative". Even the definition of consent does not include the word "affirmative".

And more generally, these so-called "rights" are not enforceable and have significant loopholes that neuter language that superficially appears to be okay.

INACCURATE, MISLEADING: And Opt-in is required for sensitive data, including location data, to ensure protection of this special class of information.

Most if not all of the other categories included in the Bad WPA's "sensitive data" clause can be inferred with high probability from non-sensitive data that is only opt-out, so there is not actually any additional "protection".

"To ensure protection" is also inaccurate. Micorosft and Amazon know that sensitive data can be inferred from non-sensitive data, so they clearly didn't put it into the bill to ensure protections. Why did they do it then?

MISLEADING: There is widespread agreement among academics and many consumer groups that opt-in for all data collection and use does not protect consumers.

Consumer Reports and Consumer Federation of America have both testified in favor of opt-in in 5062. Last year WashPIRG, Privacy Rights Clearinghouse, EFF, and EPIC Privacy all made similar points in written comments. What consumer groups oppose opt-in?

And while academics have a range of opinions about opt-in, they are almost unanimous that opt-out does not protect consumers — and consumer groups agreed.

KERNEL OF TRUTH: It's true that *by itself* opt-in does not protect consumers. 5062's approach is "notice and consent", and it's currently "notice and opt-out". If the *only* change were to make it "notice and opt-in," the protections wouldn't be any stronger in practice. And it's also true that some first-party uses of data should not require opt-in. If I'm buying something and providing my shipping address as part of it, of course I shouldn't have to opt in separately!

MISLEADING: Rather than empowering them to exercise meaningful choices, in practice it overwhelms them with consent requests and leads to notice fatigue. Consumers quickly click "accept" without thinking about each particular instance of data use to access the website or service that they want to use.

Apple begs to differ. On the iPhone, apps have to request permissions from the user. That's opt-in.

More generally, well-designed laws (like the People's Privacy Act) can minimize the number of consent requests by prohibiting secondary uses.

KERNEL OF TRUTH, FOR REAL: It is true that there are too many consent dialogs today. I'm as sick of those stupid cookie dialogs as you are. I would love to have a single browser setting that says something like "only allow cookies that are necessary to complete this transaction," knowing that they were prohibited from sharing that information, never see a cookie dialog ever again, and have stuff still work. Next time you're talking to a lobbyist from a tech company, ask them to implement that.

KERNEL OF TRUTH, OBSCURED: Many tech companies have an interest in getting users data, so do in fact (intentionally) overwhelm them with requests to wear users down.

MISLEADING: Consent is important but It is only part of the solution.

But does the Bad WPA even have meaningful consent in most places?

And do the other parts of the Bad WPA's "solution" complement consent or undercut it?.

Also, HOLD ON JUST A SECOND HERE. Consent is important, no buts about it.

INACCURATE: It should be reserved for sensitive data or sensitive uses where consumers are put in a position to exercise a meaningful choice.

"Sensitive" data can be inferred from non-sensitive data, so the sensitive/non-sensitive data distinction is meaningless.

And what are their sources for this bald assertion?

MISLEADING: The Bad WPA complements this selective use of consent with other consumer rights to control their data and by imposing affirmative duties on companies to responsible steward data.

As discussed above the Bad WPA's "rights" are not real

MISLEADING: The EU's GDPR and California Law do not require opt-in consent for all data collection and use.

California's laws are weak. There is broad agreement that GDPR is not an appropriate model for US-based privacy law.

And in any case, we now return to the original misleading framing. The question is not how the Bad Washington Privacy Act compares to other privacy law, but whether it protects Washingtonians.