Does Obama’s Online ‘Consumer Privacy Bill of Rights’ Get the Job Done?

**By** [**Matt Peckham**](http://techland.time.com/author/mcpeckham/)

The Obama administration just rolled out something it’s calling a “Consumer Privacy Bill of Rights.” It’s a first draft at this point — think of it as a blueprint for legislation down the road, a statement of principles companies can voluntarily sign onto — but given what it’s meant to do, and how it could impact future law, it’s definitely worth canvassing the key points.

CNN has [a copy of the full text of the bill](http://money.cnn.com/2012/02/22/technology/bill_of_rights_privacy/), if you want to read the preamble. I’ll summarize: It applies to personal data, which the bill defines as “any data…that is linkable to a specific individual.” That’s an over-broad definition, of course — it’s semantically linkable to pretty much *every* kind of data — but given the sensitivity of the subject matter, better to err on the side of breadth at the outset. And as the White House notes, “even without legislation, [it] will convene multistakeholder processes that use these rights as a template for codes of conduct that are enforceable by the Federal Trade Commission.”

**“Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.”** This is the bill’s first point and arguably its most important. The White House says companies “should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data.” The bill says the choices should be easy to use and access, as should our ability “to withdraw or limit consent.” While that sounds like a no-brainer, think about how byzantine or cryptic today’s company privacy strictures tend to be, whether it’s your bank, your credit card company, or the “this today, that tomorrow” mercurialness of social networks like Facebook. Many companies require you opt-out instead of opt-in, as well — I’d like to see a requirement that *all* forms of personal data sharing be opt-in and *never* opt-out, and that we place the onus on companies to sell us on the benefits of opting-in instead of hoping we never bother to check. What’s more, personal data collection practices should be front and center, not buried in the fine print or tacked on like those laughable motormouth disclosures at the end of ebullient drug company TV ads.

**“Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.”** This is the “clear and accessible” clause. The White House says “companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.” And they need to do it “[at] times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control.”

 **“Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.”** Translation: A company like Ticketmaster shouldn’t (without explicit permission, anyway) use those Bruce Springsteen tickets I just bought as license to share my information with a merchandizer like Amazon, such that the latter starts emailing me every time one of Springsteen’s albums is on sale. If companies want to use personal data for *inconsistent* purposes, the bill, in so many words, say they have a right to *ask*, but “must provide heightened measures of Transparency and Individual Choice.” And there’s a rudimentary age clause in this one that definitely needs to be fleshed out, but crucially states that “Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers.”

**“Security: Consumers have a right to secure and responsible handling of personal data.”** Simple and straightforward: Companies need to secure your data using “reasonable safeguards.” The question that’s not answered, of course, is what’s “reasonable.” For instance: Were Sony’s safeguards to the PlayStation Network “reasonable” before hacker group Anonymous broke in and absconded with millions of users’ personal information? What about the new ones Sony’s put in place since the breach? And how will this be decided legally speaking, say a data breach occurs and lawsuits ensue?

**“Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.”** This is the “how do we make sure what companies think they know about us is correct?” clause. It states that companies “should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation,” and that the principle should be construed “in a manner consistent with freedom of expression and freedom of the press.”

**“Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.”** Again, simple and obvious: Companies need to be able to justify *why* they’re collecting your personal data (and securely dispose of what they don’t or no longer use). The White House says that justification should be contingent on the “Respect for Context” clause (see above).

**“Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.”** Last but not least, this is the “we should expect companies to adhere to these principles” clause. It also says companies should “hold employees responsible for adhering to these principles” and take measures to ensure the company as a whole is in compliance.

The takeaway in two words: transparency and consistency. I’m cautiously optimistic at this stage, given the bill’s language and scope. Granted some of the points seem over-broad and could do with clarification, but as a first step, with an eye toward FTC enforcement off the block, this is a significant document, and it’s already earning subscribers: AOL, Google, Microsoft and Yahoo have already signed up.

But it won’t be just about getting companies onboard (the bill is voluntary), it’ll be about those companies figuring out *how* to comply. That’s not as straightforward as it sounds. There’s no standard Internet template for privacy mechanics (nor does the bill argue for one). One of the biggest implicit challenges here will thus be how companies structure their consumer privacy mechanics to meet the bill’s imperatives — call it the “feng shui of consumer privacy transparency.”