June 15, 2019

Poor Richard's Four Easy Steps To Compliance With the California Consumer Privacy Act (CCPA)

by Jon Neiditz

2019 is a nonstop carnival of consultants and lawyers sending you hither and thither as each new state effort to solve the purported ills of the digital world flashes its shiny omnibus bill for a moment before being dragged back into the swamp. For the moment and still likely for the rest of the year, the CCPA is your real challenge. You have been smart; you waited until the big companies with hundreds of privacy staffers asked themselves and the most expensive consulting and law firms every conceivable question. Poor Richard helped give them all the answers, and now we can boil away everything you don't need to help you, as a medium-sized business, do what you need to do. So here it is, in just four easy steps, only one of which you need to start doing now:

Obligation	Discussion of Requirement	Timeframe	How to Make This Happen

Place a "Do Not Sell My Personal Information" button on webpages. Note that "sell" under the CCPA doesn't mean sell; it means share for any benefit at all, really. So I'm going to say "share." Assume Personal Information (PI) is anything that reasonably identifies any Californian.	Put a "Please Do Not Sell My Personal Information" link on homepages, download pages for mobile apps, or pages that are otherwise collecting personal information (PI). When a consumer clicks on the "Do Not Sell" link, you can offer options (such as opting out of certain types of sharing) or just not share PI. Giving options is useful for offering choice and warning consumers of the consequences of opt-outs. Try an option not to include data transfers necessary to complete transactions to which the consumer is a party.	The button should not be placed on any websites until as late as possible, but no later than December 31, 2019. The trick is to get ready for the button with the riders discussed just below.	You must be able -- when the button goes live -- to stop the transfer of a given consumer's personal information to almost any entity that does not sign a service provider rider described below or its equivalent.

The sure way to be able to share PI when the consumer says not to is for the vendor to be a service provider, whose contract says it can't keep, use or disclose the PI for its own purposes. Poor Richard has the contract riders you need.	Yeah, Poor Richard knows you have more networked relationships than the Bigs may. But there are some critical vendors to which your sharing of PI is critical to your business. Thankfully you can leave out the "dumb pipes" that just carry stuff to your customers without extracting PI. If the critical vendors keep, use or share it for their own purposes, you need to contemplate life in which you don't share the PI of consumers who have opted out with them, or making a change.	This is the one thing you really need to start doing now, in a risk-prioritized way.	Start by identifying the critical vendors to which your sharing of PI is critical to your business, and get them service provider riders now. Then you may have to strategize about how to deal with an economy with more restrictions on sharing.
Rights Requests – Access and Deletion This is where the consultants are trying to sell you on the need to map all your data. Here's a little secret we've discovered: Probably not. But if you want, we have CCPA-focused data maps to share.	CCPA's access rights are broad, and they are likely to be the major search issues for IT if and when you get them, but by emphasizing the do-not-share button, CCPA may fous most of the action there rather than on access requests (unless you're a target). Its deletion rights, on the other hand, are full of holes, so deletion requests may result in more legal activity than IT activity. You have a 45-day clock for each.	If you think you can deal with a consumer's request for access to her PI in 45 days, we should receive all the details we'll get from the Legislature and the Attorney General by late September, so that's when to talk with IT about the 45-day access clock.	The button focuses CCPA on do-not-share rather than access or deletion, so many companies are deciding to do access manually when the time comes.

Update Privacy Policy	The CCPA requires that a business update its privacy policies to include (i) a description of consumer's rights under the CCPA, (ii) one or more designated methods for submitting CCPA rights requests, *(iii) a list of categories of personal information it has collected about consumers in the past 12 months, (iv) a list of the categories of personal information it has sold about consumers in the past 12 months, (v) a list of categories of personal information it has disclosed about consumers in the past 12 months,* and (vi) link to the "Do Not Sell My Personal Information" webpage.	This is a game of chicken where you will see lots of examples go up in December 2019 and some clarifications earlier in the Fall. You should wait to post as in any game of chicken, but should come up with what you can do to answer (iii)-(v) (immediately to the left) before then. Then, when you're ready to jump out of the car, modify in view of what similar businesses have done.	No rush and no worries, but between now and December, we should discuss how to respond to iii-v in italics at left.

Oh, and you know what to say when the consultants tell you to establish a toll-free telephone number, address employee issues, yada yada… Just don't worry about any of the stuff likely to be killed by amendments to the law. Poor Richard may travel to New York soon, and looks forward to using hand gestures in our compliance guide there.