The New York Times | http://nyti.ms/1i2T7nh

U.S. | NYT NOW

Call for Limits on Web Data of Customers

By DAVID E. SANGER and STEVE LOHR MAY 1, 2014

WASHINGTON — The White House, hoping to move the national debate over privacy beyond the National Security Agency's surveillance activities to the practices of companies like Google and Facebook, released a long-anticipated report on Thursday that recommends developing government limits on how private companies make use of the torrent of information they gather from their customers online.

The report, whose chief author is John D. Podesta, a senior White House adviser, is the next step in the administration's response to the disclosures by Edward J. Snowden, the former N.S.A. contractor that began the debate.

Because the effort goes so far beyond information collected by intelligence agencies, the report was viewed warily in Silicon Valley, where companies see it as the start of a government effort to regulate how they can profit from the data they collect from email and web surfing habits.

Mr. Podesta, in an interview, said President Obama was surprised during his review of the N.S.A.'s activities that "the same technologies are not only used by the intelligence community, but far more broadly in the public and private spheres because there is so much collection" from the web, smartphones and other sensors.

"You are shedding data everywhere," Mr. Podesta said.

The report makes six policy recommendations. They include passing a national data breach law that would require companies to report major losses of personal and credit card data, after attacks like the one on Target that exposed credit card information on roughly 70 million customers. It seeks legislation that would define consumer rights regarding how data about their activities was used. It suggests extending privacy protections to individuals who are not citizens of the United States and argues for action to ensure that data collected about students is used only for educational purposes.

But the most significant findings in the report focus on the recognition that data can be used in subtle ways to create forms of discrimination — and to make judgments, sometimes in error, about who is likely to show up at work, pay their mortgage on time or require expensive treatment. The report states that the same technology that is often so useful in predicting places that would be struck by floods or diagnosing hard-to-find illnesses in infants also has “the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education and the marketplace.”

The report focuses particularly on “learning algorithms” that are frequently used to determine what kind of online ad to display on someone’s computer screen, or to predict their buying habits when searching for a car or in making travel plans. Those same algorithms can create a digital picture of person, Mr. Podesta noted, that can infer race, gender or sexual orientation, even if that is not the intent of the software.

“The final computer-generated product or decision — used for everything from predicting behavior to denying opportunity — can mask prejudices while maintaining a patina of scientific objectivity,” the report concludes.

Mr. Podesta said the concern — he suggested the federal government might have to update laws — was that those software judgments could affect access to bank loans or job offers. They “may seem like neutral factors,” he said, “but they aren’t so neutral” when put together. The potential problem, he added, is that “you are exacerbating inequality rather than opening up opportunity.”

Edward W. Felten, a computer scientist at Princeton and former chief technologist of the Federal Trade Commission, said the goal would be for both the government and industry to address the risk of discrimination based on data analysis.

“There is a role for government to hold companies accountable and establish incentives,” Mr. Felten said. “There needs to be enough incentive for companies to do the hard work.”

Some major companies, including Google, Facebook and Microsoft, declined to comment on the report. But Michael Beckerman, president of the Internet Association, whose members include Google, Facebook, Amazon and Twitter, called the report a “useful examination” of big data technology.

Now that the report has been issued, Mr. Beckerman said, the administration should “turn its attention to the most pressing privacy priorities facing American consumers” — to update the Electronic Communications Privacy Act and to “reform

the government's surveillance laws and practices."

Other companies, including Mozilla, the maker of a popular web browser, also urged the government to focus on surveillance issues, reflecting Silicon Valley's concern that the biggest threat they face today is the suspicion around the world that the N.S.A. has built "back doors" into American products.

Google has said it will work to build encryption systems that can defeat N.S.A. spying, and several companies have revised their policies in recent months to say they will warn customers, whenever they legally can, if the government tries to subpoena data stored in their emails, in the cloud or in social media accounts. The notification would not apply in cases where a search was authorized by the Foreign Intelligence Surveillance Court, which prohibits warning targets of such searches, but the firms are clearly trying to deter the government from regularly mining their data.

In one area, the report appears to side, at least in part, with critics of the N.S.A. who argued with the intelligence agency's contention that it is far less intrusive to collect "metadata" about a phone call or email than to collect its content.

The former director of the N.S.A., Gen. Keith B. Alexander, often noted that because the agency maintained a database only of the phone numbers that Americans called and the durations of the calls, it was not violating their privacy. But the report notes that there is a "profound question" about whether that kind of metadata "should be accorded stronger privacy protections than they are currently" because they can be revealing of a person's movements and habits. "This review recommends that the government should broaden" the examination of how intelligence agencies use such data and consider whether the test should be "how much it reveals about individuals."

Mr. Podesta, in briefing reporters on Thursday, also singled out the shortcomings of the "Terms of Service" that consumers click on, almost always without reading them, when they sign up for free email accounts or download apps for their smartphones. He asked whether that process "still allows us to control and protect our privacy as the data is used and reused."

That is bound to prove contentious in the information industry, where the clicking on the terms of service is viewed as a license to use the data for a variety of highly profitable purposes.

The report also recommends extending Americans' privacy rights to foreigners, on the theory that there are no boundaries when it comes to the data collected online. Mr. Obama declared in January that the government would do the same in the treatment of

data it collects through the National Security Agency and other sources.

Marc Rotenberg, executive director of the Electronic Privacy Information Center, said that the report identified the key issues and that its policy recommendations addressed privacy groups' major concerns. "The implementation of those proposals," Mr. Rotenberg said, "is the big challenge now, what happens next."

David E. Sanger reported from Washington and Steve Lohr from New York.

A version of this article appears in print on May 2, 2014, on page A1 of the New York edition with the headline: Call for Limits On Web Data Of Customers.

Next in U.S.
A Late Rush to Sign Up for Insurance