June 17, 2013 6:13 pm

Make privacy part of the transatlantic trade talks

By Yochai Benkler

Time to address the threat from the public-private partnership for surveillance, says Yochai Benkler

©Dreamstime

One of the US constitution's great strengths is its strong protection for privacy against government intrusion. One troubling feature, therefore, of the recently revealed collaboration between the National Security Agency and America's global information providers is that the government has found a way to bypass the constitution. It uses weaknesses in legal protections that, in both the US and Europe, are intended to allow private companies to keep records on their clients while shielding citizens from prying by their governments.

American law privileges consumer sovereignty over human dignity, so it provides weak privacy protection against snooping by companies. They may create extensive dossiers on customers, and because they provide services globally but have systems anchored in the US, those data are subject to American government observation as well.

But, in US law, privacy is historically more robust when it comes to the government's right to create similar dossiers. The kind of dragnet surveillance of phone metadata that the order to Verizon exposed would, in normal times, have triggered forceful resistance. It is similar to the undirected search warrants deployed by the British in their North American colonies – an injustice that inspired the fourth amendment, which offers protection against unreasonable searches.

In the response to the September 11 2001 attacks, many constitutional bulwarks were breached. Torture, indefinite detention, eavesdropping on journalists or aggressive prosecution of their national security sources – these are not the American constitutional way. Objections are repeatedly waved away. "You're talking as though 9/11 never happened," we are told. The US has almost recovered from the most

vicious manifestation of this malaise – the Bush-Cheney torture programme. But indefinite detention continues and the Bush-Obama surveillance system is thriving. Even in normal times, however, US constitutional law is concerned with Americans and American soil. Foreigners abroad are not subjects of concern; invasion of their privacy is collateral damage. What can citizens on both sides of the Atlantic do to address the threat from this public-private partnership for surveillance?

Some things we can all do. Just as we have learnt to make ethical consumption choices to address environmental concerns, so too we must educate ourselves in using tools that will protect us. We must use strong encryption and pick genuinely secure communications and storage technologies.

Europeans, for their part, can put pressure on the private side of the collaboration to cut the flow of data into the public-private surveillance system. The EU is considering revising its data protection directive to make it easier for companies to collect and use data in ways more similar to those common in the US. This is the result of a close alliance of interests between government surveillance and the marketing interests of the companies involved; it will require sustained political pressure in Europe to prevent it.

Unfair data practices should also be part of negotiations over the new trade agreement between the US and the EU. They are fundamentally like unfair labour practices: the party with weaker standards gives its domestic players an advantage in data-driven marketing at the expense of the core human value of privacy. The congruence between the self-interest of European companies and the privacy interests of European and US citizens may provide sufficient political heft to tamp down on commercial practices that make user data readily available for abuse.

With the surveillance programme anchored on the western side of the ocean, it will be up to Americans to mobilise around these revelations. Already there are cries for a fundamental re-evaluation of our intelligence operations. A left-right coalition of civil liberties advocates and libertarians has emerged.

There may be trade-offs and hard choices where privacy and security are concerned. But the secrecy of the programmes has long prevented all but inside specialists from discussing them. We need to find out how many Americans are willing to give up how much of their liberty in exchange for what level of security and at what level of transparency.

Each time details emerge about programmes adopted in the post-9/11 constitutional panic, such as torture or indefinite detention, they expose the assurances of their critical value as vacuous at best, and usually duplicitous. We need a transparent debate for our own sakes. In having it, we will be doing our bit to help innocent subjects caught in the dragnets of US programmes around the world.

The writer is a professor at Harvard Law School and a director of the Berkman Center for Internet & Society