COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Privacy & Data Security

November 27, 2013

EUROPEAN COMMISSION ISSUES SIX POINT POLICY RESPONSE TO U.S. SURVEILLANCE PROGRAMS; SUPPORTS REFORM OF U.S.-EU SAFE HARBOR

On November 27, 2013, the European Commission issued a press release, together with several memos, outlining a policy response to media revelations about the alleged impact of U.S. surveillance and intelligence programs on the privacy of European citizens. The response consists primarily of six separate "action points," which are designed to "rebuild trust" in flows of personal data between the EU and the U.S. The six points are summarized in more detail below.

In summary, the European Commission response advocates acceleration of reform of European data protection laws and the quick finalization of a Trans-Atlantic treaty on police and law enforcement access to data; proposes new reforms to the U.S.-EU Safe Harbor data transfer mechanism; and recommends new measures for the U.S. Government that would amend existing U.S. laws and extend new protections to European citizens.

I. THE COMMISSION'S SIX POINT POLICY RESPONSE

- First, the Commission argues that the proposed reform of European data protection laws — as would be implemented by the General Data Protection Regulation and accompanying Directive — should be fast-tracked and adopted before "spring 2014."
- Second, the Commission has completed its review of the U.S.-EU Safe Harbor (a process that was started by Commissioner Viviane Reding in mid-July this year). The Safe Harbor is the legal mechanism used by many U.S. companies to transfer data from Europe to U.S. headquarters for processing. The review ended in the conclusion that "the current implementation of the Safe Harbor cannot be maintained" and resulted in 13 proposed amendments, which the Commission now plans to implement "by summer 2014." The 13 proposals — which represent a reform of the Safe Harbor, rather than its abandonment — are summarized further below in this e-alert.
- Third, the Commission recommends that ongoing negotiations for an umbrella treaty for transfers and processing of police and law enforcement data be concluded quickly, in order to ensure that citizens of both the U.S. and EU receive equal protections in relation to requests for law enforcement data. (Trans-Atlantic negotiations over the proposed treaty agreement began in 2010.)
- Fourth, the Commission proposes that the U.S. Government should embrace the use of Mutual Legal Assistance Treaties (MLATs) and other sector-specific agreements (*i.e.*, including Passenger Name Records Agreement and Terrorist Financing Tracking Programme) when making requests for companies to turn over data to law enforcement agencies. This would help companies avoid being put in a position where complying with a request from one jurisdiction would force them to break non-disclosure requirements and data protection laws in another.

- Fifth, the Commission has advocated that the U.S. should extend to European citizens any new protections that result from President Obama's ongoing review of the authority of U.S. national security agency powers in a manner that equally protects the rights of Europeans, as well as Americans.
- Sixth, and finally, the Commission has proposed that the U.S. should accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as "Convention 108"). Convention 108 is regarded as the most influential international instrument of data protection law and was a forerunner to the European Data Protection Directive of 1998.

II. PROPOSAL TO REFORM THE SAFE HARBOR

One of the memos that accompanied the Commission's press release was the result of a Commission assessment of the U.S.-EU Safe Harbor mechanism. As mentioned above, instead of abandoning the Safe Harbor mechanism, the Commission has now proposed 13 new amendments in a memo that accompanies the press release described above; each is summarized below.

Enhanced Disclosure

1. Companies that self-certify with the Safe Harbor should be required to publicly disclose their privacy policies. Currently, the Commission notes that many companies only provide the U.S. Department of Commerce with a description of the privacy policy — but nevertheless collect data from online sources without providing full clarity with a privacy policy on their own websites. The Commission says this is not sufficient and that company privacy policies, particularly with regard to the collection of online data, should be made "publicly available on the companies' websites, in clear and conspicuous language."
2. Such privacy policies should be required to include a link to the Department of Commerce list of "currently certified" members of the Safe Harbor. This change would make it easier to verify whether a company's certification is current or lapsed (although it is possible, if less easy, to verify this at present), but is not really new, as the Department of Commerce already began to ask companies to do this following March 2013.
3. If a company that is certified with the Safe Harbor enters into *any* contracts with subcontractors, the Safe Harbor terms should require those companies to publish the "privacy conditions" of the terms of those subcontracting agreements. This would, according to the Commission, push companies to "make public the privacy safeguards" employed by companies when subcontractors are used.
4. Companies whose certifications have lapsed should be identified as having failed to comply with the Safe Harbor requirements more clearly, rather than simply being identified as having a "not current" certification. This would help act as a clearer warning to data subjects about the dangers of lapsed certifications.

Enhanced Redress Mechanisms

1. Publicly available company privacy policies should be required to include links to alternative dispute resolution (ADR) processes that are relevant to the Safe Harbor certification. This is again a change introduced by the Department of Commerce in March 2013 that the Commission wishes to "accelerate" to all Safe Harbor members.
2. Safe Harbor certified companies should make ADR "readily available and affordable." All companies certified to the Safe Harbor are already required to make ADR available to

complainants, under the "Enforcement" Principle of the U.S.-EU Safe Harbor, and Department of Commerce guidance already recommends that such mechanisms be "readily available and affordable." However, the Commission notes that complaints made to Data Protection Panels (an option made available in cooperation with European regulators) are free, unlike some other ADR methods that can be used.

3. The Department of Commerce should "more systematically" review the transparency, accessibility, and procedures of Safe Harbor ADR providers, including in order to check on how the ADR providers follow up on complaints. The Commission recommends that any breaches found by the Department of Commerce also be published, in order to punish non-compliant ADRs (by showing Safe Harbor companies, who choose ADR providers, which ADR providers are most effective at resolving disputes).

Enforcement of the Safe Harbor

1. A percentage of certified companies — unspecified by the Commission at this time — should be made subject to ex officio investigations, which dig deeper than "control of compliance with formal [Safe Harbor] requirements." The details of this new investigation regime have yet to be specified, however.
2. When companies are found non-compliant under the newly proposed inspection regime, the Commission proposes that a follow-up investigation be performed "after 1 year." Such an inspection would presumably be automatically mandated.
3. The Department of Commerce should notify the relevant European data protection authority whenever doubts are raised as to the compliance of a company with the Safe Harbor requirements. The Commission has yet to detail this new notification requirement, and it is not yet clear whether the Department of Commerce would want to be bound by a requirement to notify the relevant European authority or whether it would merely do so on a voluntary basis.
4. Any claims made by companies that are not Safe Harbor certified should be investigated robustly. This recommendation is meant to prevent companies from falsely claiming compliance with the Safe Harbor framework — although it is unclear how common this problem is right now in practice.

Access to Data by U.S. Government Enforcement Authorities

1. Companies certified with the Safe Harbor should be required, in their privacy policies (which are to be made public under the first Commission recommendation above), to "include information on the extent to which U.S. law allows public authorities to collect and process data transferred under the Safe Harbor. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements." This proposed requirement is not yet detailed, and it is currently unclear whether, under this proposal, companies would be required to do much more than (i) disclose the existence of relevant U.S. laws, (ii) describe those laws (iii) and exemptions that may apply under those laws to prevent disclosure, and finally (iv) explain which, and perhaps how frequently, exemptions may apply.
2. Lastly, the Commission also notes that it is "important" that the Safe Harbor national security exception — which permits the disclosure of Safe Harbor data transferred to the U.S. for "national security" purposes — be used only to an extent that is "strictly necessary or proportionate." The Commission does not currently provide any further details on the conditions that could be applied to determine whether any specific transfer, or set of transfers, is in fact necessary or proportionate or how or who would make this determination in respect of a transfer.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our international privacy and data security practice:

Daniel Cooper	+44.(0)20.7067.2020	dcooper@cov.com
Henriette Tielemans	+32.(0)2.5495252	htielemans@cov.com
Kurt Wimmer	+1.202.662.5278	kwimmer@cov.com
Monika Kuschewsky	+32.(0)2.549.5249	mkuschewsky@cov.com
Mark Young	+44.(0)20.7067.2101	myoung@cov.com
Ezra Steinhardt	+44.(0)20.7067.2381	esteinhardt@cov.com