10-20-2014

Sweeping Claims and Casual Legal Analysis in the Latest U.N. Mass Surveillance Report

Peter Margulies

LAWFARE

FISA

Sweeping Claims and Casual Legal Analysis in the Latest U.N. Mass Surveillance Report

By **Peter Margulies** Monday, October 20, 2014, 4:11 PM

Privacy Paradox: Rethinking Solitude

U.N. Special Rapporteur Ben Emmerson's report on "mass surveillance" may signal increasing conflict between the US and world bodies on surveillance issues. The Emmerson report makes sweeping normative claims but fails to ground those claims in an accurate description of the US surveillance program. The report claims, for example, that a state must impose the same restrictions on surveillance of foreign nationals overseas that it imposes on surveillance of its own citizens within sovereign territory. Universal state practice clashes with this claim. Furthermore, no tribunal, domestic, regional, or international, has ever embraced such a sweeping limitation. Emmerson's document makes a valuable point on the need for independent checks on surveillance, but its casual legal analysis and cavalier posture on facts undermine its value.

The first problem with the Emmerson piece is its failure to include widely available factual descriptions of US surveillance that rebut the report's findings. Take the excellent U.S. Privacy and Civil Liberties Oversight Board (PCLOB) report on § 702 of the Foreign Intelligence Surveillance Act, which governs U.S. surveillance overseas. The Special Rapporteur suggests that US surveillance abroad, such as surveillance authorized by § 702, constitutes illegal "mass surveillance." However, the Emmerson report does not incorporate the PCLOB's extensive discussion (at pp. 32-36), of the nuanced nature of § 702 surveillance.

While Special Rapporteur Emmerson suggests that the US indiscriminately collects communications off the Internet's backbone, the United States' approach is far more tailored. The text and structure of § 702 require targeted surveillance, not indiscriminate collection. Surveillance methods have to be approved by the Foreign Intelligence Surveillance Court (FISC); persons targeted include those working with international terrorists, such as ISIS, international nuclear weapons dealers, and individuals evading sanctions that the US and global bodies have imposed on terrorists. (Section 702 also permits targeting that serves the "foreign affairs" of the US, a less concrete category. Congress should consider refining this category, as I say in a forthcoming Hastings Law Journal paper on § 702, although the largest use of this category may be targeting of foreign governments and firms that engage in anti-competitive practices.)

Emmerson's analysis also gives an incomplete account of the law governing transnational surveillance. Let's bracket an issue on which the Special Rapporteur and I agree that the U.S. is wrong: the extraterritorial effect of the International Covenant on Civil and Political Rights (ICCPR). Accepting the ICCPR's extraterritorial application, Article 17 of the ICCPR requires merely that interference with privacy not be "arbitrary" or "unlawful." To avoid arbitrariness, a practice needs to be grounded in a rational purpose, free from whim or bias. To be lawful, a practice needs to be grounded in state law and provide those affected by the practice with general notice that they may be subject to the practice. The ICCPR therefore gives states a qualified right to engage in surveillance to further national security and law enforcement, as long as this interference is not indiscriminate or invidious, is consistent with state law, and provides citizens with a modicum of transparency.

Unfortunately, the Emmerson report emulates the disregard of treaty language displayed by both the U.N. Human Rights Committee and ICCPR commentator Manfred Nowak. Instead of recognizing the flexibility that the drafters of the ICCPR accorded to states by including the term, "arbitrary," the report inserts a proportionality requirement for surveillance that the text does not mention. The attempt to supplement treaty language with new terms and understandings outside of the agreement's text is a staple of European human rights treaty interpretation. However, it clashes with Article 31(1) of the Vienna Convention on Law of Treaties, which requires interpreters to first consult the "ordinary meaning" of a treaty's text. While Article 17 may incorporate some type of proportionality analysis, it does so only in the obvious sense that arbitrariness will likely characterize government means that are grossly disproportionate to ends. That perfunctory nod to proportionality reflects a far more deferential standard than the one that the U.N. report adopts.

Even accepting that proportionality should play a role in interpreting Article 17, the report's proportionality standard fails to incorporate the deference that the European Court of Human Rights (ECHR) has required regarding the European Convention's Article 8. That provision is stricter than the ICCPR, because it permits only "necessary" interference with privacy. In *Weber v. Germany*, the ECHR gave states substantial latitude in conducting surveillance abroad on wrongdoers, noting that states lacked the ability to enforce their laws directly on people overseas. As a result, surveillance of criminals and security threats abroad was often the least restrictive means available to keep citizens safe. The Emmerson report's requirement that states use identical standards for domestic and international surveillance ignores the ECHR's wisdom. The report also devotes only passing mention to states' duty under U.N. Security Council Resolutions, such as SC Res. 2178, to prevent terrorist groups from "exploiting technology, communications, and resources." Individual states may be unable or unwilling to comply with this duty regarding activity within their borders; transnational surveillance by other states can bridge the gap.

Ironically, the Emmerson report's insistence on identical standards for domestic and international surveillance actually sabotages efforts to protect privacy. States are most likely to try innovative measures to protect privacy when these measures protect state nationals within the state's territory. If those measures also keep the homeland safe, a state may well expand them to include aspects of international surveillance. Enforcing a

lockstep approach to domestic and international surveillance chills that experimentation.

Similarly, the report rejects the use of "delegated legislation" that allows the legislative, executive, and judicial branches of government to tailor surveillance to national security and law enforcement needs without undue disclosure (Para. 43). Delegated legislation may allow states to restrain executive decisions through legislative oversight and judicial review, even when the public lacks detailed knowledge of particular surveillance programs. The Emmerson report's rejection of this approach hinders the cause of accountability.

Its insistence on public disclosure also departs from ECHR case law. In *Weber*, the ECHR acknowledged that public disclosure of criteria for surveillance could lead to terrorist suspects and others "adapting their conduct" by staying just below the surveillance threshold. Moreover, the *Weber* Court recognized that notice to targets of surveillance could undermine the purposes of investigation. The Emmerson report fails to grapple with the ECHR's guidance.

A more helpful report designed to increase dialogue would have proceeded in a different fashion. Careful analysis would have been welcome on the role of limits on government access to and use of personal data. As I've noted in my recent paper on § 702, technology isn't merely a sword to pierce individual privacy; it's also a shield to prevent government analysts from gaining access to data that doesn't further security or law enforcement needs. Search filters, automated monitoring of analysts' compliance with search protocols, and other measures can discipline national security bureaucracies. The FISC has required such methods for several years. A careful look at the utility and reliability of such use restrictions might have advanced dialogue immeasurably. So could a discussion of differences between "collect[ing] all communications or metadata all the time indiscriminately," which the Emmerson piece appears to claim that the US does, and scanning portions of the Internet backbone to reveal particular identifiers linked to terrorists, which the US actually does. This automated scanning does not result in the collection of all content, and the NSA has disclosed the elaborate ways in which it limits analysts' access to irrelevant data. A careful report could have addressed these practices, and suggested refinements to add additional layers of privacy protection. Safeguards of this kind might have informed the "arguable justification for mass surveillance" that the Emmerson report acknowledged was possible "in principle" (Para. 34).

Emmerson did perform a valuable service by reminding nations of the importance of independent checks on surveillance. While the FISC is independent (in contrast with weaker *ex ante* checks on surveillance in most other countries, including the UK), FISC review could be even more robust (see the excellent post by Steve and Marty). The bill sponsored by Senator Patrick Leahy with the support of the Obama administration is a good start, permitting the FISC to name *amici curiae* who could argue against the government's position on novel legal issues. The Leahy bill also mandates certification of such issues to higher courts. However, the Leahy bill's safeguards do not establish the robust institutional presence that a public advocate at the FISC would supply. Moreover, as I noted in my Hastings piece, certification may not produce the diligent judicial review that surveillance reformers desire, since certification has been resisted by courts for decades.

A commitment to more robust external checks would enhance the credibility and legitimacy of US transnational surveillance programs. As Ashley Deeks has noted in an insightful article on surveillance and human rights, independent checks will likely increase in importance in coming years. If the US had such checks in place, drafters of future U.N. studies might feel obliged to describe US practices more precisely than the U.N. Special Rapporteur does in his latest report.

Topics: FISA, Surveillance: Snowden NSA Controversy, FISA: 702 Collection, Privacy, FISA: Reform, FISA: 215 Collection, Internet Metadata Collection, Surveillance

---

Peter Margulies is a professor at Roger Williams University School of Law, where he teaches Immigration Law, National Security Law and Professional Responsibility. He is the author of Law's Detour: Justice Displaced in the Bush Administration (New York: NYU Press, 2010).