This panel discussion is on private and multi-stakeholder efforts to curtail government hacking of civilian targets.

Governments are increasingly asserting the authority to compel communications service providers. For example, the United Kingdom and Australia recently adopted legislation that confers authority on government officials to seek assistance from communications service providers and device manufacturers in accessing communications that might otherwise be protected against access by technological means. Companies are pushing back with important initiatives like the Cybersecurity Tech Accord, in which company signatories pledge not to assist governments with cyber attacks on innocent civilians and companies, as well as the call for a “Digital Geneva Convention.”

Government hacking and company responses raise a number of important issues for consumers, firms and policymakers. These include the mechanics of how commitments not to assist governments in conducting cyberattacks against civilian targets will be implemented. They also include issues of transparency and accountability to internet users to ensure that they understand what protections they do and do not enjoy and that they understand available avenues for redress. Finally, these policies raise questions about how states will react, and whether they will accept refusals from firms in the event that the state seeks private sector assistance.

The panel discussion, co-organized by the Center for Democracy and Technology, the Internet Governance Lab at American University, and the Cyber Governance and Policy Center at the University of Oklahoma, will feature a gathering of company stakeholders, advocates and scholars.