The Algorithmic State: Cyber Challenges to Democracy

Roundtable: Friday, Dec 11, 8:30-13:00 (by invitation only).

The goal of the roundtable is to identify some of the challenges in cyber policy for innovation, civil rights and security, and to discuss different strategies for addressing them. The structure will be fully participatory (Chatham House Rules).

09:00-11:00 — PPI (Public-Private Interface)

The algorithmic state is deeply interfaced with the private sector. Basic state functions, such as policymaking, law enforcement, ensuring public safety and national security, are now partially implemented through the use of algorithms, often involving technologies, data sources, data analytics and infrastructure developed, operated or owned by the private sector. Consequently, individual developers and private companies may be called upon to carry out tasks or to engage in actions previously part of the domain reserve of the sovereign state. Therefore, the relationships between the state and private actors reflect a complex web of interdependencies: states operate by using technologies, data and infrastructure of private actors, sometimes developed with the intended purpose of protecting against state intrusion, and at the same time the state is also expected to protect private infrastructure, data and technologies. In the post-Snowden era, some tech companies seek to limit collaboration with state authorities. Yet the increasingly-blurred distinction between public/private is challenging both specific legal rules and the theoretical principles that underlie the rule of law. In this digital ecosystem, the state could shape the cyber security landscape by a variety of tools, such as procurement, standard setting, regulation, and law enforcement. Several questions arise from these new developments:

- Is PPI indeed a "partnership"?
- Is the state co-opting the industry to act as its long arm, or is the industry co-opting the regulator?
- What models of collaboration are available for public/private cyber collaboration?
- Are these models satisfactory for meeting the cyber challenges (enhancing security, ensuring basic liberties)?
- Are these models addressing the needs of the private sector?
- Can they sufficiently ensure competition and innovation?
- What legal rules are governing PPI in various jurisdictions? Do they fit PPI in cyber?

11:00-13:00 — Checks and Balances

In the emerging cyber ecosystem, premised on robust surveillance and algorithmic analysis, and offering innovative yet potentially dangerous offensive and defensive tools, issues of misuse, capture and social control arise. Current checks-and-balance structures may be ill fitted to address such concerns. Therefore:

- How should we think about appropriate checks and balances to ensure that the new algorithmic cyber technologies are not misused by either the state or industry?
- Which institutional structure could ensure restrain of dynamic algorithmic governance that is based on constant change and machine learning?
- How do we ensure that the guardians are guarded, where transparency is unavailable?
- What types of domestic institutions and procedures do we have in place to review both the state and the industry with which it interfaces?
- How best to address potential agency-principle problems and other types of conflict of interests?
- How best to enlist the transnational and international regimes in order not only to empower states but also to curtail misuses of their powers, given the inherent principle-agent problems?
- What type of technological "checks" should we envision?

13:00-13:30 — Concluding Remarks

Professor Jonathan Zittrain, George Bemis Professor of International Law, Harvard Law School | Harvard Kennedy School of Government, Professor of Computer Science, Harvard School of Engineering and Applied Sciences, Co-Founder, Director, and Faculty Chair, Berkman Center for Internet & Society

Prof. Isaac Ben Israel (Maj-Gen. (Res.)), Director of the Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University

The Algorithmic State:
Cyber Challenges to Democracy

Around The Table
(Partial List)

- **Adv. Amit Ashkenazi,** Legal Adviser, The Israel National Cyber Bureau
- **Prof. Gad Barzilai**, Dean Faculty of Law, University of Haifa
- **Ms. Eva Beyvers**, DFG Research Training Group "Privacy", University of Passau, Germany
- **Prof. Isaac Ben Israel** (Maj-Gen. (Res.)), Director of the Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University
- **Prof. Michael Birnhack**, The Buchmann Faculty of Law, Tel Aviv University
- **Mr. Ami Braun**, Senior Vice President, Comsec Group
- **Mr. Niv David**, Research fellow, Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel-Aviv University.
- **Prof. Orr Dunkelman** - Department of Computer Science, University of Haifa
- **Prof. Niva Elkin-Koren**, Director, Haifa Center for Law & Technology, University of Haifa
- **Dr. Eldar Haber**, Berkman Center for Internet & Society, Harvard University and Minerva Center for the Rule of Law Under Extreme Conditions, University of Haifa
- **Dr. Kenneth Geers**, Ambassador for the NATO Cyber Centre in Estonia, Visiting Professor University of Kyiv
- **Prof. Dr. Gerald Spindler**, Department of Commercial Law and IT-Law, Göttingen University
- **Adv. Yoram HaCohen**, CEO, Israel Internet Association
- **Adv. Deborah Housen-Couriel,** Minerva Center for the Rule of Law Under Extreme Conditions, University of Haifa | Interdisciplinary Cyber Center, Tel Aviv University | Konfidas Digital Ltd.

- **Dr. Jeanette Hofmann**, Director of the Humboldt Institute for Internet and Society
- **Mr. Erez Kreiner**, CEO, Cyber-Rider
- **Mr. Ram Levi**, CEO - Konfidas Digital Ltd.
- **Dr. Chris Parsons**, SSHRC Postdoctoral Fellow, Citizen Lab, Munk School of Global Affairs | Managing Director, Telecom Transparency Project
- **Mr. Shuki Peleg**, Head of Cyber Defense and Information Security - First International Bank of Israel (FIBI)
- **JUDr. Radim Polcak**, Ph.D, Institute of Law and Technology, Masaryk University
- **Prof. Amnon Reichman**, Minerva Center for the Rule of Law Under Extreme Conditions, Faculty of Law, University of Haifa
- **Prof. Joel Reidenberg**, Director of the Center on Law and Information Policy, Fordham University
- **Mr. Danny Rosenne**
- **Mr. Ido Rosenzweig**, Director of Research (Cyber, Terrorism and Belligerency), Minerva Center for the Rule of Law Under Extreme Conditions, University of Haifa
- **Prof. Eli M Salzberger,** Director, Minerva Center for the Rule of Law Under Extreme Conditions, Faculty of Law, University of Haifa
- **Dr. Tehila Shwartz Altshuler**, Israel Democracy Institute
- **Prof. Nico Van Eijk**, Director, Institute for Information Law (IViR) Faculty of Law, University of Amsterdam
- **Mr. Lior Yoffe**, The Israel National Cyber Bureau
- **Prof. Tal Zarsky**, HCLT, University of Haifa
- **Prof. Jonathan Zittrain,** George Bemis Professor of International Law, Harvard Law School | Co-Founder & Director, Berkman Center for Internet & Society