ASAF LUBIN
1 Chauncy St., Apt. 17, Cambridge, MA, 02138
asaf.lubin@yale.edu || asaf.lubin@gmail.com || 254-722-1979

TEACHING AND RESEARCH INTERESTS

Primary Interests: Insurance Law, Privacy Law, International Law, Torts Law, Law and Technology (especially Cybersecurity Law)

Secondary Interests: Conflict of Laws, National Security Law, Human Rights Law, Criminal Procedure, International Business Transactions

EDUCATION

YALE UNIVERSITY, SCHOOL OF LAW, J.S.D. **(expected, 2019)**
Dissertation: "The Law on Espionage: From Unilateral Agencies to Multilateral Mechanisms Governing the International Law of Intelligence" (W. Michael Reisman, supervisor)
Honors: Robert L. Bernstein International Human Rights Fellowship (2016-2017)
Kennedy's Prize for Best Conference Presentation, Kings College London (2016)
Raphael Lemkin Prize for Best Paper in the field of Human Rights Law (2018)
Activities: Member, Yale Law School Fellowships Working Group (2017-2018)
Resident Fellow (2015-2018), Visiting Fellow (2018-2020), Information Society Project
Visiting Scholar, Hebrew University Federmann Cybersecurity Research Center (2017-2020)
Co-Chair, Fifth, Seventh, and Eight Annual Doctoral Scholarship Conference (2015, 2017, 2018)
Yale Society of International Law (Scholarship and International Mooting Chair) (2015-2016)
International Community at YLS (Co-founder and Graduate Programs Advisor) (2017)
Philip C. Jessup International Law Moot Court Competition; Nelson Mandela World Human Rights Moot Court Competition; Charles Rousseau International Law Moot Court Competition; Hague International Monsanto Tribunal Project (Coach and Team Advisor) (2016-2018)
Graduate Teaching Fellow, Modern Hebrew Department, Yale University (2015-2016)
Yale Law and Technology Society (VP Community Outreach) (2015-2016)

YALE UNIVERSITY, SCHOOL OF LAW, LL.M. **(2015)**
Honors: Decalogue Society of Lawyers Endowment for LL.M. studies in the field of Social Justice (2014)
Activities: "*Intelligence Law*" Reading Group, Information Society Project (developed and co-led) (2015)
Salzburg Global Seminar, Lloyd Cutler International Law Fellowship (Washington D.C.) (2015)
Yale Journal of International Law (YJIL) (articles editor) (2015)

HEBREW UNIVERSITY OF JERUSALEM, LL.B., B.A. International Relations, *magna cum laude* **(2013)**
Honors: Fritz & Margaret Oberlander Memorial Award in International Law (2012)
Abraham Spears Endowment for Excellence in an International Moot Court Competition (2012)
The Lamas Fund, Hebrew University Rector Award for Advanced Legal Studies Abroad (2014)
Activities: Israel Law Review (under the auspices of Cambridge University Press) (student editor) (2010-2011)
Philip C. Jessup International Law Moot Court (participant, coach, national administrator) (2011-2014)

THE HAGUE ACADEMY OF INTERNATIONAL LAW, Public International Law Summer Programme **(2012)**
Honors: Professor Shabtai Rosenne Scholarship (merit-based, full-tuition award)

PROFESSIONAL EXPERIENCE

AFFILIATE, BERKMAN KLEIN CENTER FOR INTERNET AND SOCIETY
Harvard University, 2019-2020

CYBERSECURITY POLICY POSTDOCTORAL FELLOW, FLETCHER SCHOOL OF LAW AND DIPLOMACY
Tufts University, 2018-2019

EXPERT, UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)
United Nations, 2018-2019

ROBERT L. BERNSTEIN HUMAN RIGHTS FELLOW, LEGAL TEAM
Privacy International (London), 2016-2017

RESEARCH ASSISTANT TO PROFESSOR JACK GOLDSMITH
Internet and U.S. National Security Course (Yale Law School), 2016

RESEARCH ASSISTANT, REISS CENTER ON LAW AND SECURITY
Global Intelligence Oversight Project (NYU), 2015

CLERKSHIP, OFFICE OF THE LEGAL ADVISOR
Israeli Ministry of Foreign Affairs, 2013-2014

RESEARCH ASSISTANT TO JUSTICE (RET.) JACOB TURKEL
The Public Commission of Inquiry to Examine the Maritime Incident of 31 May 2010, 2011-2013

INTERN, OFFICE OF THE PROSECUTOR (UN-ICTY OTP)
United Nations International Criminal Tribunal for the Former Yugoslavia, 2012

PUBLICATIONS AND WORKS IN PROGRESS

***The Insurability of Cyber Risk* (Job Talk Paper)**
Increased economic risk from cyber-attacks has led to the rise of cyber insurance as a means for risk prevention and management. Stand-alone cyber insurance policies now offer coverage for an array of cyber risks affecting the private and public sectors, which include both first party harms (such as a business interruption and network shutdown triggered by an attack on third-party suppliers or cloud-service providers) and third party harms (such as costs for notification and credit monitoring services and legal fees associated with data breaches of users' information). In June 2017, the food and beverage conglomerate *Mondelez International* became a victim of the NotPetya ransomware attack with tens of thousands of its servers and computers becoming inoperable causing over $100 million in losses. Zurich American Insurance informed Mondelez in 2018 that cyber coverage, not explicitly mentioned in Mondelez's all-risk property insurance policy, would be denied based on the "war exclusion clause." This case, now pending, will be a watershed moment for the cyber insurance industry, highlighting the great ambiguity around the insurability of certain types of cyber risk and the scope of coverage that insurers will provide in the case of a cyber incident. The paper argues for technology-neutral regulation of the cyber insurance market. Relying on traditional insurance and torts jurisprudence, specifically the literature on public policy and insurable exposure, the paper makes the case for the indemnification of four controversial categories of cyber harm: (1) acts of cyber terrorism or state-sponsored cyber operations; (2) extortion payments for ransomware attacks; (3) administrative fines for violations of statutory data protection regulations; and (4) disruption to supply, service, or distribution chains. In doing so, the paper highlights systemic challenges to cyber insurance underwriting while proposing limited regulatory solutions to ensure that cyber insurers play a proactive role in increasing cyber posture among their policy holders while reducing the likelihood of moral hazards.

Journal Articles

***Cyber Insurers and Cyber Constables: Strange Bedfellows?*, 10(1) J. NAT'L. SEC. L. & POL'Y (forthcoming, 2019)**
Underwriters play a growing role in *ex ante* modeling of cybercrime risks for actuarial purposes, and *ex post* cyber forensic analysis for claims investigations. In doing so they are becoming an important piece in the cybercrime prevention puzzle, contracting out to cybersecuirty experts and firms, including form the intelligence and law enforcement sector. At the

same time, however, insurers can also interfere with the crime prevention efforts of law enforcement. By indemnifying ransom payments, they incentivize victims of cyber attacks to pay off hackers and criminals, indirectly supporting the ransomeware industry. Similarly, by covering costs associated with fines and liabilities from violations of certain data protection regulations, they increase the likelihood of moral hazards, thereby weakening those regulations' deterrence value. This paper examines these tensions and discusses policy and legal reforms necessary to ensure a better collaboration between insurers and law enforcement in the criminal administration of cyber norms.

***The Liberty to Spy*, 61(1) HARV. INT'L. L.J. (forthcoming, 2019)**

Many, if not most, international legal scholars share the ominous contention that espionage, as a legal field, is devoid of meaning. The notion that international law is moot as to the question of if, when, and how intelligence is to be collected, analyzed, and promulgated, has been repeated so many times that it has attained the status of a dogma. This paper offers a new and innovative legal framework for articulating the law and practice of interstate peacetime espionage operations, relying on a body of moral philosophy and intelligence ethics thus far ignored by legal thinkers. This framework adopts a diagnosis of the legality of covert intelligence, at three distinct temporal stages – before, during, and after. In doing so it follows the traditional paradigms of international law and the use of force, which themselves are grounded in the rich history of Just War Theory. Adopting the *Jus Ad*, *Jus In*, *Jus Post* model makes for an appropriate choice, given the unique symbiosis that exists between espionage and fundamental U.N. Charter principles. This paper, focuses on the first of the three paradigms, the *Jus Ad Explorationem* (*JAE*), a sovereign's prerogative to engage in peacetime espionage and the right's core limitations. Examining a plethora of international legal sources the paper exemplifies the myriad ways by which peacetime intelligence gathering has been already recognized as a necessary pre-requisite for the functioning of our global legal order. The paper then proceeds to discuss the nature of the *JAE*. It argues that that the right to spy is best understood as a privilege in Hohfeldian terms. It shows how understanding interstate intelligence operations as a weaker "liberty-right" that imposes no obligations on third parties to tolerate such behavior, helps capture the essence of the customary norms that form part of the practice. The paper concludes by discussing case studies to exemplify those practices which may be considered as abusing the right to spy.

'*We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18(2) CHI. J. INT'L L. 502 (2018) (*Winner of the 2018 Yale Law School Raphael Lemkin Prize for Best Paper in the field of Human Rights Law*)

Intelligence agencies have been recently involved in the exercise of global indiscriminate surveillance, which purports to go beyond their limited territorial jurisdiction and sweep in "the telephone, internet, and location records of whole populations." When called out about any of these programs, policy makers often respond to their constituencies with a shrug and a smile: *'we only apply these programs to foreigners, you have nothing to worry about'*. While the human rights community continues to adamantly uphold the myth of a universal right to privacy, in actuality the *pax technica* has already erected an alternative operational code, one in which "our" rights to privacy and "theirs" are routinely differentiated. One higher set of standards and protections is provided for those within the territory of the state, and a lowered set is handed to those abroad. This distinction is a common feature in the wording of electronic communications surveillance regimes and the practice of signals intelligence collection agencies, and it is further legitimized by the steadfast support of the layman general public. Nonetheless, a liberal defense of this distinction is non-existent in the literature, as human rights scholars continue to oppose it arguing that it reflects in-group biases and violates the principle of non- discrimination. In this piece I try to make the liberal case for the distinction, justifying, in a limited sense, certain legal differentiations in treatment between domestic and foreign surveillance. These justifications, as I show in the piece, are grounded in practical limitations in the way foreign surveillance is conducted, both generally and in the digital age more specifically. I will further make a controversial claim: that in fighting this absolutist battle for universality, human rights defenders are losing the far bigger war over ensuring some privacy protections for foreigners in the global mass surveillance context. Accepting that certain distinctions are, in fact, legitimate, creates an opportunity to step outside the bounded thinking of one-size-fits-all human rights standards for all surveillance practices, and begin a much needed conversation on what a uniquely tailored human rights regime might look like in the foreign surveillance context. This piece, thus, makes a first attempt at sketching out such a tailored framework, with the hope of bridging the divide between privacy scholars and national security practitioners.

***The Dragon-Kings Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum*, 57 WASHBURN L. J. 17 (2018)**

The U.S. and China are at it again, as naval and aerial interceptions in and around the South China Sea become a matter of disturbing routine. At the heart of the dispute stands the lingering question of whether customary international law as

reflected in the United Nations Convention on the Law of the Sea (UNCLOS) authorizes third State to engage in surveillance and military maneuvers in Coastal states EEZ without their consent. The answer lies in interpreting Article 58(1) of UNCLOS. This paper aims to respond to the calls put forward by States, scholars and research institutes to promote a legal compromise between permissive and prohibitive interpretive approaches to UNCLOS Art. 58(1). The traditional interpretation of the Article, and the EEZ Surveillance conundrum more broadly, has thus far been reviewed by scholars solely through the lenses of the age-old debate between Hugo Grotius and John Selden over Mare Liberum and Mare Clausum. In other words, existing scholarship treats the dispute as a binary zero-sum game. Following in the footsteps of Prof. Lissitzyn, the model proposed in the Article recognizes the freedom of navigation premise as an analytical starting point, but nonetheless introduces, for reasons of maintaining minimum order, a set of restraints ("necessity," "last resort," and "proportionality") to be internalized by third States' in deciding whether to launch intelligence operations in another coastal State's EEZ. To develop these standards the paper examines the limits of a State's right to spy under international law and the effects that advancements of surveillance technology have had over our evolutionary interpretation of UNCLOS. The paper's nuanced approach thus treats the EEZ surveillance problem as a microcosm through which to examine meta-issues concerning the function intelligence plays in our public world order.

***Hacking for Intelligence Collection in the Fight Against Terrorism: Israeli, Comparative, and International Perspectives*, 13 HUKIM L. REV. (forthcoming, 2019) (in Hebrew)**

The Counter-Terrorism Bill, 5775-2015, introduced an array of criminal law and public law tools aimed at assisting the State of Israel in effectively fighting against terrorism. Simultaneously, the Bill sought to ensure a balance between the security interests, enumerated therein, and Israel's commitments to "human rights and to customary international legal standards". Of the various tools introduced in the Bill, Section 131 was one of the most controversial, as it called to amend the General Security Service Law, 5762-2002, and provide the Shabak with statutory authorization to engage in hacking of electronic devices for the purposes of preventing acts of terrorism and espionage directed against the State of Israel. The desire of the Israeli legislator to expressly regulate the authorities of the Shabak in cyberspace, reflects a growing trend amongst western democracies to establish, through primary legislation, effective frameworks that could control the use of hacking powers by intelligence agencies and law enforcement. The paper examines existing and proposed Israeli hacking authorities and compares them to the situation in the United States, the United Kingdom, Italy and France. Relying further on international human rights standards, the paper makes certain policy and legislative recommendations.

Book Chapters

***The Rights to Privacy and Data Protection under IHL and HRL*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW (KOLB, GAGGIOLI & KILIBARDA eds., 2nd ed., forthcoming, 2020)**

To date, there is little international humanitarian law (IHL) scholarship or ICRC legal opinion around the nature and scope of application of the right to privacy, and its supplementary modern right to data protection, in times of armed conflict. Given the developments in communication and surveillance technologies of the last two decades this seems to be a glaring and startling omission. The two rights thus make an excellent case for the study of the potential concurrent application of IHL and international human rights law (IHRL). This chapter tries to identify the normative foundation for the existence of the rights to privacy and data protection in times of war focusing predominately on our ability to draw guidance from IHRL. After proving the existence of the rights in times of war, the chapter shifts the focus to discuss their particular scope of application in specific privacy infringing wartime practices, including the data protection obligations of a belligerent occupier towards the civilian population in the occupied territories; the rights of POWs, detainees, refugees, and those internally displaced over their electronic devices and data stored in the cloud; the restrictions imposed on wartime SIGINT collection for aerial targeting and offensive cyber-attacks; and the obligations imposed on international organizations and Courts in the collection of digital evidence for jus post bellum criminal investigations.

***Politics, Power Dynamics, and the Limits of Existing Self-Regulation and Oversight in ICC Preliminary Examinations*, *in* 2 QUALITY CONTROL IN PRELIMINARY EXAMINATIONS: REVIEWING IMPACT, POLICIES, AND PRACTICES 77 (MORTEN BERGSMO & CARSTEN STAHN ed., 2018)**

Should the normative framework that governs the International Criminal Court's (ICC) oversight concerning Preliminary Examinations (PE) undergo a reform? The Chapter seeks to answer this question in the affirmative, making the claim that both self-regulation by the Office of the Prosecutor (OTP) and quality control by the Pre-Trial Chamber (PTC) currently suffer from significant deficiencies, thus failing to reach the optimum point on the scale between absolute prosecutorial discretion and absolute control. The Chapter relies on the 2015 Palestinian referral in order to demonstrate some of these inadequacies. The Chapter first maps out the legal structures and mechanisms that currently regulate the PE stage. The

Chapter then proceeds to explore a number of key areas where the OTP has considerable independence, and concerning which sufficient quality control is critical to ensuring the legitimacy of the PE process, and of the Court itself. This review includes an analysis of the potential for politicization of the Court, the problems faced by the OTP when attempting to articulate generalized prioritization policies and exit strategies, the regulation of evidentiary standards at the PE stage, and the role of transparency in the PE process. The Chapter concludes with four suggestions for potential reform of the control mechanisms over prosecutorial discretion in the PE process: (1) re-phasing of the PE phase and the introduction of a Gantt-based review process; (2) redefinition of the relationship between the OTP and PTC at the PE stage; (3) redrafting of existing OTP policy papers on PEs and Interests of Justice and the adoption of a new policy paper on evidence and evidentiary standards; and (4) introducing a "Committee of Prosecutors" as a new external control mechanism.

Works in Progress

Examining the Anomalies, Explaining the Value: Should the USA Freedom Act's Metadata Program be Extended? **(with Professor Susan Landau) (in progress)**

The telephony metadata program which was authorized under Section 215 of the PATRIOT Act, remains one of the most controversial programs launched by the U.S. Intelligence Community (IC) in the wake of the 9/11 attacks. Under the program major U.S. carriers were ordered to provide NSA with daily Call Detail Records (CDRs) for all communications to, from, or within the United States. The Snowden disclosures and the public controversy that followed led Congress in 2015 to end bulk collection and amend the CDR authorities with the adoption of the USA FREEDOM Act (UFA). For a time, the new program seemed to be functioning well. Nonetheless, three issues emerged around the program. The first concern was over high numbers: in both 2016 and 2017, the Foreign Intelligence Surveillance Court issued 40 orders for collection, but the NSA collected hundreds of millions of CDRs, and the agency provided little clarification for the high numbers. The second emerged in June 2018 when the NSA announced the purging of three years' worth of CDR records for "technical irregularities." Finally, in March 2019 it was reported that the NSA had decided to completely abandon the program and not seek its renewal as UFA is set to sunset in December 2019. This paper sheds significant light on all three of these concerns. First, through careful analysis of the numbers, we provide a guide for how forty orders might lead to the collection of several million CDRs, thus offering a model to assist future researchers in understanding transparency reporting from the IC across its various surveillance programs. Second, relying on the architecture of modern telephone communications, we provide possible technical explanation for the 2018 purge. Finally, we show how changes in the terrorist threat environment as well as in the technology and communication methods they employ — in particular the deployment of asynchronous encrypted IP-based communications — has made the telephony metadata program far less beneficial over time. We further provide policy recommendations for Congress so to advance its ability to offer effective intelligence oversight in the future.

Blind Oracles: Regulating Intelligence Gathering, Analysis, and Verification for Wartime Aerial Strikes **(submitted for review, AM. J. INT'L L.)**

The potentially catastrophic effects of faulty intelligence assessments are perhaps at their starkest in the context of wartime aerial attacks. Modern history is filled with examples of wartime intelligence errors that resulted in calamitous air campaigns. The paper examines twelve such cases from the Battle of Monte Cassino in Italy during World War II (15 February 1944) through Operation Allied Forces Bombing of the Chinese Embassy in Belgrade (7 May 1999) to the Israeli Gaza Beach Attack during Operation Protective Edge (14 July 2014). The paper makes the claim that faults in wartime intelligence processing, analysis, and verification are not as inevitable as often presumed, and that it is for a lack of regulation within the treatises of IHL, that they occur at the rate that they do. Tribunals and military manuals guide us to rely on the "reasonable commander test" in determining the lawfulness of a particular strike. Yet, in the process we overlook the fact that any reasonable commander will turn to her "reasonable intelligence analyst" - the contours of this standard are conspicuously under-defined. This paper takes a first step at proposing such an international standard, basing such regulatory guidelines on both historical analysis and emerging soft-law norms in the field of wartime intelligence production.

PROFESSIONAL ESSAYS AND ONLINE PUBLICATIONS

The International Law of Rabble-Rousing (with Hendrick Townley) (45(1) YALE J. INT'L L. ONLINE 1, (forthcoming, 2019))

Expert Opinion on Questions on Comparative Privacy Law and Data Protection Regulation and Related Conflict of Laws Issues, Class Action (Tel Aviv) 62205/17 *Lior Winter and Liraz Spector v. Google Israel Ltd. and Google LL.C.*, (2 January 2019) (at the request of Shapira Bar-Or Matzkin & Co. Law Offices)

C*yber Law and Espionage Law as Communicating Vessels*, PROCEEDINGS OF THE 10TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT, CYCON X: MAXIMISING EFFECTS, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDCOE) (2018)

Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements, LAWFARE (23 April 2018)

A *Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens*, 42(2) YALE J. INT'L L. ONLINE 1 (2017)

A Roadmap for the Cross-Border Data Transfers Debate, Hebrew University of Jerusalem Federmann Cybersecurity Research Center Blog (15 September 2017)

Foreign Surveillance and Anti-Discrimination: The Justifications for Applying Different Safeguards for Extraterritorial Surveillance, Hebrew University of Jerusalem Federmann Cybersecurity Research Center Blog (19 August 2017)

Its Time to Open Substantive Discourse Over Judicial Oversight for Drone Strikes, THE PAVLOVIC TODAY (30 June 2017)

Israeli Airstrikes in Syria: The International Law Analysis You Won't Find, JUST SECURITY (3 May 2017)

European States Pushing for Unbridled Retention of Its Citizens' Data, THE REAL NEWS NETWORK (30 January 2017)

A New Era of Mass Surveillance is Emerging Across Europe, JUST SECURITY (9 January 2017)

The Investigatory Powers Act and International Law, UCL J. L. & JURIS. BLOG (26 December 2016)

25 Reasons Why All Law Students Should Participate in the Jessup Competition, UCL J. L. & JURIS. BLOG (30 September 2016)

Espionage as a Sovereign Right Under International Law and its Limits, 24(3) ILSA Q. 22 (2016).

***Technology and the Law on the Use of Force: New Security Challenges in the Twenty-First Century (by Jackson Maogoto)*, Book Review**, 40(2) YALE J. INT'L. L. 441 (2015)

Alice Through the Looking Glass: Operational Debriefings, Temporal Delimitations, and Commissions of Inquiry, The Emil Zola Chair for Human Rights, Judicial Decisions Highlight No. 37 (2014) (in Hebrew)

TEACHING EXPERIENCE

LECTURER, YALE UNIVERSITY
Espionage and International Law (designed and taught a 13-week undergraduate course), 2017, 2018

TEACHING ASSISTANT TO PROFESSOR W. MICHAEL REISMAN

Public Order of the World Community Course (Yale Law School), 2017, 2018, 2019

LEAD INSTRUCTOR, YALE YOUNG GLOBAL SCHOLARS
Yale University, 2015-2019

TEACHING ASSISTANT TO PROFESSOR DAVID KRETZMER
Terrorism, Counter-Terrorism, and Human Rights Course; *Public International Law Course*; *The Laws of Armed Conflict Course* (Hebrew University of Jerusalem and Sapir College of Management), 2013-2014

TEACHING ASSISTANT TO PROFESSOR TOMER BROUDE
Legal Writing and Research Course (Hebrew University of Jerusalem), 2011-2012

ADDITIONAL INFORMATION

Languages: Hebrew (native), English (native)

Certifications: Certificate of College Teaching Preparation (CCTP), Yale Center for Teaching and Learning; Certificate in Data Protection, The British Computer Society (BCS)

Memberships: American Society of International Law, American Bar Association Section of International Law, European Society of International Law, Global Commission on the Stability of Cyberspace (Law Section of the Research Advisory Group).

CONFERENCES AND LECTURES (2017-2019)

New York University Law School, Selected Presenter, Cyber Enforcement Symposium: Author's Workshop, "*Cyber Insurers and Cyber Constables: Strange Bedfellows?*" (June 2019)

Privacy Law Scholars Conference (PLSC), UC Berkley Law School, "Examining the Anomalies, Explaining the Value: Should the USA Freedom Act's Metadata Program be Extended?" (together with Susan Landau) (June 2019)

Harvard Kennedy School, Belfer Center for Science and International Affairs, Invited Panelist, "*The Ethics and Morality of Espionage*" (May 2019)

Tufts Tech and Data Industry Night, Invited Panelist, "*What's the Price of Paying Attention?*" (April 2019)

World Summit on the Information Society, United Nations, Invited Panelist, "*Cybersecurity and AI: How to allocate the liability between the various stakeholders?*" (April 2019)

Boston University, Rafik B. Hariri Institute for Computing and Computational Science and Engineering, Cyber Security, Law, and Society Alliance, Invited Speaker, "*How Private Insurers Regulate Public Cybersecurity?*" (April 2019)

Naval War College, Lectures of Opportunity, Invited Speaker, "*The Liberty to Spy*" (February 2019)

Hebrew University of Jerusalem, The Federmann Cybersecurity Center, Cyber Law Program, Cyber Lunch, "*Private Insurers as Regulators of Data Protection and Cybersecurity Practices*" (January 2019)

Hebrew University of Jerusalem, International Law Forum, "Israel and International Law: Developments and Patterns in the Year 2018," Invited Panelist, "*Europe's New Normal: Foreign Mass Surveillance and the Jurisprudence of the European Court of Human Rights*" (December 2018)

Hebrew University of Jerusalem, The Federmann Cyber Security Center, Cyber Law Program Workshop, "*Conflict of Laws and the Information Society*" (December 2018)

Fletcher School of Law and Diplomacy, Institute for Business in the Global Context, Invited Moderator, "*Counterterrorism Surveillance Law and Practice: A Deep Dive with Clint Watts*" (November 2018)

Harvard Law School, Program on International Law and Armed Conflict, Advocates for Human Rights, Harvard International Law Journal, and Harvard National Security Journal, Invited Speaker, "*Tinker, Tailor, Lawyer, Spy: Espionage and International Law*" (November 2018)

Fletcher School of Law and Diplomacy, The Fletcher LL.M. Program in International Law, Invited Speaker, "*The International Law of Cyberespionage*" (October 2018)

Yale Law School, Public Order World Community, Invited Speaker, "*Espionage and International Law*" (October 2018)

NATO Cooperative Cyber Defence Centre of Excellence, 10th International Conference on Cyber Conflict (CyCon), "*Cyber Law and Espionage Law as Communicating Vessels*" (May 2018)

Yale Naval Reserve Officers Training Course (NROTC) Leadership Conference, Workshop Leader, "*Espionage and International Law*" (April 2018)

Yale International Relations Symposium, Invited Speaker, "*Human Rights and International Law*" (April 2018)

American Society of International Law (ASIL), 112th Annual Meeting, New Voices Panel, "*The Sovereign Right to Spy*" (April 2018)

The Innovation Center for Law and Technology at New York Law School and the High Tech Law Institute at Santa Clara University School of Law, Internet Law Works-in-Progress Conference, "*Comity and the Information Society*" (March 2018)

Yale Information Society Project, Workshop Co-organizer and Panel Moderator, "*Extraterritorial Enforcement: Developing Norms for the Information Society*" (March 2018)

American Society of International Law (ASIL), Midyear Meeting, "*Blind Oracles: Regulating Intelligence Gathering, Analysis, and Verification for Conducting Wartime Aerial Strikes*" (October 2017)

Institute for International Law of Peace and Armed Conflict, Ruhr-Universität Bochum, Invited Discussant, "*Young International Law Workshop*" (October 2017)

Hebrew University of Jerusalem, Faculty of Law, The Centre of Legislation and Comparative Law in the name of Hari and Michael Saker, Roundtable discussion on Law and Cyberspace, "*Hacking in the Fight Against Terrorism: Israeli, Comparative, and International Perspectives*" (June 2017)

Centre for International Law Research and Policy (CILRAP), The Hague Peace Palace, "*Politics, Power Dynamics, and the Limits of Existing Self-Regulation and Oversight in ICC Preliminary Examinations*" (June 2017)

Hebrew University of Jerusalem, Faculty of Law, Cyber Security Research Center, "*Regulation of Communication Networks Surveillance and the Principle of Proportionality*" (June 2017)

Privacy Law Scholars Conference (PLSC) Europe, Tilburg Institute for Law, Technology and Society, TILTING Perspectives, "*We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Extraterritorial Mass Surveillance*" (May 2017)

NYU Center for Global Affairs in Collaboration with U.N. Security Council's Counter Terrorism Committee's Executive Directorate, Roundtable Discussion on UNSC Resolution 2322, Invited Discussant, "*International Cooperation and Downgrading Intelligence*" (April 2017)

Westminster Law School, International Law at Westminster Law Series, "*The International Law of Peacetime Espionage*" (April 2017)

Michigan Law School Third Annual Young Scholars' Conference, "*We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Extraterritorial Mass Surveillance*" (March 2017)

Queen Mary University Law School, LL.M. Program, "International Law and Intelligence Collection" (March 2017)

Essex University, Roundtable Discussion with Civil Society, Invited Discussant, "*The Investigatory Powers Act*" (January 2017)

Cambridge University, MPhil International Relations Course, "*The Ethical Spy: Espionage in the Province of the Law*" (January 2017)

Oxford University, Future of Humanity Institute, "*The Surveillance State and the Future of Humanity*" (January 2017)

REFERENCES

Professor John A. Burgess
Fletcher School of Law and Diplomacy, Tufts University
(617)-627-2521; john.burgess@tufts.edu

David O'Brien,
Berkman Klein Center for Internet and Society, Harvard University
(617)-495-7547; dobrien@cyber.harvard.edu

Professor James J. Silk
Yale Law School
(203)-432-1729; james.silk@yale.edu

Professor Yuval Shany
Faculty of Law, Hebrew University of Jerusalem
+972-2-588-2541; shany.yuval@gmail.com

Professor W. Michael Reisman
Yale Law School
(203)-432-4962; michael.reisman@yale.edu

Professor Matthew Waxman
Columbia Law School
(212)-854-0592; mwaxma@law.columbia.edu

Caroline Wilson Palow
Privacy International
+44(0)7538976609; caroline@privacyinternational.org

Professor Edward (Ted) Wittenstein
Jackson Institute for Global Affairs, Yale University
(203)-436-5946; edward.wittenstein@yale.edu