THE ISRAEL DEMOCRACY INSTITUTE

מרכז המחקר להגנת הסייבר
CYBER SECURITY RESEARCH CENTER

האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

Israel and international on-line surveillance standards

Yuval Shany

International Covenant on Civil and Political Rights, 1966 - Art 17(1)

- No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Working Draft Legal Instrument on Government-led Surveillance and Privacy

- Draft initiated by UN Special Rapporteur on the Right to Privacy
- Presented in March 2018 to Human Rights Council
- Combination of hard law and soft law
- Strives to give content to “arbitrary interference standard”
  - UN HRC – GC 35(2014) “The notion of “arbitrariness” is not to be equated with “against the law”, but must be interpreted more broadly to include elements of inappropriateness, injustice, lack of predictability and due process of law, as well as elements of reasonableness, necessity and proportionality”

Arbitrariness concerns:
No legal basis

- Draft article 3 - No surveillance, domestic or foreign, civil or military, may be carried out except by a law 379 enforcement agency (LEA) or a Security and Intelligence Service (SIS) or any public-mandated 380 entity (PME) tasked by a specific law.

Israel's on-line surveillance law: Deficient legal basis

- Generality of legal framework – Basic Law: Human Dignity and Liberty, Protection of Privacy Law 1981 (official authority exception, security database exception)
- Partiality of legal framework –
  - Communications Data Law 2007 (no application to ISA)
  - ISA Law 2002 (gathering of metadata)
- Outdatedness of legal framework –
  - Wiretapping Law, 1979 (the public conversation exception) – covering also data and metadata
- Use of secret regulation –
  - Secret rules issued by PM under article 11 of ISA Law to regulate the transfer of metadata from telecommunication companies to ISA
  - Secret rules issued by PM/MoJ under article 9B of the Wiretapping Law

Arbitrariness concerns: Specific legal powers

- Draft article 4:

(1) States shall provide that surveillance systems shall be authorised by law prior to their use. This law shall – a. identify the purposes and situations where the surveillance system is to be used; b. define the category of serious crimes and/or threats for which the surveillance system is to be used; c. state that the agency using the surveillance system should only use the system in cases where a reasonable suspicion exists that a serious crime may be committed or a genuine threat to security exists; d. define and provide the least intrusive measures which potentially might be suitable to achieving the aim; e. demand from the authority to justify that each single measure envisaged is necessary and proportionate for the obtaining of vital intelligence in an individual operation as well as considering the overall impact of this and such measures on the right to privacy of persons irrespective of whether this is a citizen or resident of that state

Israel's on-line surveillance law: Lack of specificity

- Basic Law – limitation clause
- Protection on Privacy Law – The legal authority defence, the security exception
  - **19.** (a) No person shall bear responsibility under this Law for an act which he is authorized to do by Law.
    (b) A security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for the purpose of performance thereof.
- Wiretapping Law – ISA Power to monitor on *national security grounds* specific persons or *facilities* (bulk collection) and public conversations (data mining); no clear definition of data retention powers

Israel's on-line surveillance law: Lack of specificity

- ISA Law – art. 11: Metadata necessary for the ISA for fulfilling its functions under the law; no clear definition of data retention powers
- Communication Law – art. 13: PM authorized to order installing communication devices or technological adjustment of communication devices if needed for performance of functions by security forces
- Protection of Privacy Regulations (Transfer of Information) – art. 2: Transfer on grounds of public order or safety

Arbitrariness concerns: Application to concretely defined cases

- Draft article 3(9) - Any surveillance activity must only be carried out for concretely defined specific and legitimate purpose and in response to a concrete and legitimate need
- Draft article 4(10) - provide that the deliberate monitoring of an individual's behaviour or other information by the State should only be targeted surveillance carried out on the basis of reasonable suspicion

Israel's on-line surveillance law: Sweeping legal powers

- Areas of legal *lacuna* or significant uncertainty
  - Collection of OSINT and data mining
  - Bulk collection
  - Territorial application of surveillance authority and safeguards
  - Definition of metadata (location, websites)
  - Limitations on encoding/backdoors/Trojans
  - Data retention by private and public entities
  - Cellular location tracking

Arbitrariness concerns:
Lack of adequate safeguards

Draft article 3:
These safeguards shall include but shall not be restricted to a system of checks and balances consisting of: a. Legislative oversight on a regular basis and at least quarterly, by a Committee of the regional or national elected legislative body responsible for the entity funding and tasked for the purpose by law, of the budgetary and operational performance of all LEAs, SIS and PMEs authorized by law to carry out surveillance, both domestic and foreign, with the authority to temporarily or permanently withhold, suspend, grant or cancel the funding of any surveillance program or activity; b. A Pre-Authorisation authority, completely independent from the entity and the executive or legislative branches of government, composed of one or more members with the security of tenure of, or equivalent to, that of a permanent judge which is tasked by law to evaluate ex-ante requests from and grant permission to LEAs, SIS and PMEs as shall be required under law prior to the conduct of lawful surveillance; c. An Operational Oversight authority, completely independent from the entity, the Pre-Authorisation Authority and the executive or legislative branches of government, composed of one or more members with the security of tenure of, or equivalent to, that of a permanent judge which is tasked by law to exercise ex-post oversight over and exercise accountability of LEAs, SIS and PMEs as shall be required under law especially for the conduct of lawful surveillance; d. Inter-institutional whistle-blower mechanisms that allow for anonymity of the whistle blower(s), protection from retaliation and include extra-authoritarian and/or extra institutional review of the process including remedies; e. The presentation and publication of reports, at minimum on an annual basis, by the Legislative, Pre-Authorisation and Operational Oversight Authorities

Israel's on-line surveillance law: Lack of adequate safeguards

- Lack of 'double lock' system of pre-authorization in national security cases under the Wiretapping Law (Ministerial review/no review in urgent cases); periodic updating of AG; annual review by a parliamentary committee
- No annual reporting beyond 2012 to Parliament on application of the Communications Data Law
- Judicial review for police metadata applications is in place, but approval rate is more than 99.8% (like judicial approval rate for wiretapping applications)
- No need for warrant for interagency metadata transfers (under Communications Data Law and ISA Law)
- Not clear what oversight provisions exist with respect to metadata collection by ISA
- No surveillance oversight authority

Arbitrariness concerns:
Lack of remedies

- Draft article 9 - States shall provide that where a surveillance system or non-surveillance data is used for surveillance purposes, the individual subject of the surveillance, whether directly or incidentally, has a right to notification.

- Draft Article 11 - Everyone whose rights and freedoms as set forth in this legal instrument are violated shall have an effective remedy before an authority notwithstanding that the violation has been committed by persons acting in an official capacity.

Israel's on-line surveillance law: Lack of remedies

- Exemption from duty to allow database inspection under Protection of Privacy Law to security databases – impacting the associated rights of amendment and erasure;
- No duty of notification
- Rules on inadmissibility of evidence gathered in breach of the Wiretapping Law

- General administrative law/constitutional law remedies

Arbitrariness concerns: Indications of Abuse

- Under Communications Data Law - Number of police applications almost tripled between 2008-2016; percentage of location data almost doubled during the period; number of urgent non-judicial warrants quadrupled
- Media reports on extensive use of surveillance powers in the West Bank
- Media reports of request by PM to monitor top clearance officials

Other legal standards

- Right to human assessment (draft article 9)
- Right to appeal (draft article 10)
- Prohibition on profiling (draft article 3(10)
- Intelligence sharing (draft article 4(5))
- Limited data retention period (draft article 4(1)(l))
- Independent surveillance oversight authority (draft article 4(1)(m))
- Periodic transparency reports (draft article 4(2))
- Impact assessment for new surveillance systems (draft article 5-6)
- Prohibition on use of intelligence for purpose other than produces (draft article 7)
- Need to ensure security (draft article 12)

IDI Policy Recommendations

- Modern surveillance legislation
  - Regulation of ISA Bulk Collection/non-specific interception
  - Regulation of data retention
  - Rights of data subject – notification, erasure, remedy
  - Regulation of data mining
  - Regulation of transfer of information from ISP
  - Regulation of interception powers of data/metadata
- Increased specificity and transparency in regulation
- Stronger independent institutional oversight
  - Subjecting security wiretapping/interception to independent authority
  - Stronger judicial review – special advocates, minimization procedures
  - Expanding power of Protection of Privacy Authority or establishing new oversight authority + ombudsman
  - Enhanced parliamentary oversight