Secret surveillance and personal data protection: moving forward

May 24, 2013

Surveillance and interception – the status quo

A recent case of a secretly recorded, intimate video footage being released online – apparently from within the administration – in order to discredit a reporter claiming to possess incriminating information against governmental officials once again highlighted severe shortcomings in the area of privacy protection and illegal surveillance.

It is positive that, in this case, the government launched an investigation: a deputy Minister of Interior has been arrested in connection with the case and the authorities have committed to destroying an archive of personal and intimate recordings that were apparently collected in recent years to potentially discredit or blackmail people of public life.

However, it is now necessary to also address other systemic violations and shortcomings in the protection of people's right privacy, which is key to a free and democratic society. Reporters, like many other professions, need to be able to rely on the confidentiality of their electronic communication with their sources. Systematic surveillance thus poses a threat to civil liberties, including freedom of the media.

'Black boxes' for systematic, electronic surveillance

- The Ministry of Interior maintains 'black boxes' in the server infrastructure of all major telecommunication companies.
    - These black boxes allow law enforcement bodies and security services to monitor all communication passing through the system, including text messages, internet traffic and phone calls.
    - According to telecom insiders, the authorities have the technical capacity to monitor 21,000 mobile phone numbers at the same time.
    - This real-time monitoring is done through a direct connection; no further assistance from telecom companies is needed.
    - We believe the direct access to citizens' communication data has been systematically abused and that, in practice, there is no or insufficient court oversight over this surveillance.

A lack of court oversight and a weak culture of accountability of law enforcement and intelligence bodies creates a strong risk that direct access to communication data is abused and that journalists, civil society activists, politicians or members of the business community against have their movement and communication monitored.

By law, the use of intercepts is subject to authorization by a judge. However, judges are typically not informed in depth about the subject matter of the investigation and are not told the results of the surveillance. In the past, judges have rubber-stamped prosecutors' applications for surveillance and communication interception. It is not clear to what extent this is still the practice.

The Ministry of Internal Affairs and its special operations and intelligence departments have been lacking accountability for a number of years. There appears to be de facto no oversight over the activity of intelligence services through Parliament. This has led to a situation where law enforcement and intelligence services – or people affiliated with these organizations – were apparently involved in politically motivated illegal surveillance.

Publicly known cases include:

- Reporters, including from Batumelebi and TV9, who faced attempts of blackmail and coercion based on illegal surveillance;
- The reported blackmailing of the female assistant of a Tbilisi City Court judge in December 2012 with intimate, secretly obtained records;
- The posting of secretly recorded conversations between members of the Georgian Dream on YouTube in September 2012;
- The reported infiltration of computers of the Georgian Dream campaign team and the Ivanishvili family through trojans and spyware, resulting in the release of private and secretly taken pictures ahead of the October 2012 elections.

A representative of the Georgian Ministry of Interior affairs appears to be permanently located at the office of Georgian National Communications Commission (GNCC), the telecom and broadcasting regulator. The MIA representative is not actively involved in the activity of GNCC but apparently questions staff about their duties and obligations. The GNCC is an independent regulatory organization and outside interference is forbidden. The permanent presence of MIA representative there raises concerns about possible interference.

Moving forward: Improve oversight, create transparency

Oversight

- **Law enforcement:** The government should establish a strong oversight mechanism for surveillance and communication data retention by law-enforcement bodies. This oversight mechanism should have sufficient resources and enjoy a high level of independence from the executive branch of government.
    - The mandate of the new personal data commissioner and his office, which is currently established based on the Law on Personal Data Protection, could be extended to include cases related to criminal investigations, which are exempted from the mandate, as are issues related to national security.

- A team of legal experts located in the office of the personal data commissioner could receive the mandate to scrutinize any applications, renewals and cancellations of intrusive surveillance by law-enforcement bodies and conduct sampling monitoring of how surveillance is implemented in practice.

- **Intelligence:** Parliament should establish appropriate oversight over the work of intelligence services and establish a new culture of accountability. A parliamentary commission could take on the role of monitoring of the general conduct of intelligence agencies, including their use of surveillance and wiretapping.

Data collection

The Ministry of Interior should remove its *Black Boxes* from the infrastructure of telecommunications companies. The existence of direct, unlimited access to peoples' communications data undermines the concept of independent court oversight over interception and creates an intrinsic risk for abuse.

- Law enforcement should only be granted access to data after acquiring a court approval (w/ exceptions as defined by law), and access should be limited to the persons, numbers, topics and time period covered by the court approval. Furthermore, any access to telecommunication data through this system should be documented to track potential abuse.
- The government should not outsource surveillance activities to mobile operators and Internet service providers but develop a process for obtaining data in consultations with the judiciary, operators and the GNCC that is fully in line with the spirit of the law and that contains sufficient safeguards to prevent systematic, unchecked access to user data.

Transparency

- The Ministry of Justice or Ministry of Interior should regularly and proactively release aggregate information about the number of cases in which surveillance is applied, the number of applications rejected by courts, the type of surveillance used, the duration of these efforts, the aggregate number of individuals affected and the articles of the criminal code under which this surveillance measures were approved.
- The Ministry of Interior should be open about the government's communications data retention. The public has a right to know if and what telecommunications data is collected, how it is collected and stored by the authorities and how long such data is retained.

The G-MEDIA program is made possible by support from the American people through USAID. The content and opinions expressed herein are those of Transparency International Georgia and do not reflect the views of the U.S. Government, USAID or IREX.