Giuseppe Stefano Quintarelli
Member of Parliament of the Republic of Italy
Civici e Innovatori
stefano@quintarelli.it

cc: Stefano Aterno
Studio Legale Aterno
stefano@aterno.it

March 29, 2017

Re: Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali

Dear MP Giuseppe Stefano Quintarelli,

On February 15, 2017, Civici e Innovatori published a legal proposal with a framework for the government's use of hacking tools, such as trojans and other software designed to extract data from internet-connected devices and systems. The notice explained that 45 days would be provided for the public to comment on the proposal.

Access Now thanks Civici e Innovatori for pursuing a legal framework for hacking and thanks you for your work drafting the framework. We are submitting this comment to provide feedback on specific details of the proposal and their impact on individual human rights and to request additional information be made available to the public to better understand the Italian government's current hacking activities and how they may be impacted by the provisions in this proposal.

Access Now is an international civil society organization that defends and extends the digital rights of users at risk around the world. The Access Now policy team furthers Access Now's mission by developing and promoting rights-respecting practices and policies. We seek to advance laws and global norms to affect long-term systemic change in the area of digital rights and online security, developing insightful, rights-based, and well-researched policy guidance to governments, corporations, and civil society.

In addition, our tech team provides technology solutions and real-time advice for users at risk in circumstances where communications are not open, free, or safe. Through our 24/7 Digital Security Helpline, we offer technical guidance and incident response to inform and support activists, journalists, human rights defenders, and civil society actors on the ground.

I. Government Hacking and Human Rights

In 2016, Access Now published, "A Human Rights Response to Government Hacking," a policy report examining the types and applications of government hacking activities and their impact

on human rights.[1] The report, which was the result of extensive coordination and consulation, defined hacking as the manipulation of software, data, a computer system, network, or other electronic device without the permission of the person or organization responsible for that software application, data, computer system, network, or electronic device, and/or without the permission or knowledge of users of that or other software, data, computers, networks, or devices ultimately affected by the manipulation.

We indicated that more information is necessary to determine the full scope and impact of government hacking on human rights, but based on the information available we concluded that there should be a presumptive prohibition on government hacking. However, based on the size and scale of current operations we also concluded hacking is likely to become increasingly prevalent and therefore we called for governments to limit their hacking activities to those engaged in for surveillance purposes, and in those instances to implement legal frameworks to protect human rights.

Finally, the document examines exactly what elements a legal framework should include. We set out ten human rights safeguards for government hacking, which include elements such as a process for reporting vulnerabilities, purpose limitations for hacking operations, and necessity for approval by a judge who is provided with both sufficient detail and technical expertise to understand the full implications of the application.

II. Italy's Proposed Framework

The law proposed in Italy was drafted to provide a framework for the use of "trojan horses," defined to mean hidden software, "install[ed] and use[d], on personal devices, without the user's knowledge...to collect evidence for investigation."[2]

While Access Now does not condone government hacking activity, as explained above, we believe it is of pivotal importance that if it is to be conducted, it is done within a robust legal framework.

We agree with Civici e Innovatori that searches conducted through hacking are significantly different than traditional searches and that a framework tailored to hacking operations is needed to take into account relevant unique features. This framework must be "consistent with constitutional guarantees" in Italy, but we believe it must also comply with Italy's human rights obligations.[3] For this reason we provide the below comments on both general and specific ways to ensure that the law properly protects human rights.

---

[1] https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf (hereinafter "A Human Rights Response to Government Hacking").
[2] The translations in this document were provided for Access Now by Diego M. Cantoni with our great appreciation.
[3] http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-pdl-captatori-IT.pdf at 2 (hereinafter, "Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali").

A. *General Observations*

i. Transparency

> *"Agencies conducting government hacking should publish at least annually reports that indicate the extent of government hacking operations, including at a minimum the users impacted, the devices impacted, the length of the operations, and any unexpected consequences of the operation."*[4]

In a two-pager meant to provide more information on the proposal, Civici e Innovatori indicates that "[f]or some years, the judiciary has been ordering remote digital extractions of data and remote interceptions of face-to-face conversations."[5] Unfortunately there is very little publicly-available information on previous government hacking activities by Italian government officials. The software used by Italian government officials includes grossly invasive features, including the ability to activate a camera and take photos, modify or insert information, turn on the microphone, and access external archives.[6] Without greater transparency on if and how these capabilities are utilized it is difficult to substantively comment on the adequacy of the proposed law with regard to ensuring that any previous deficiencies are being specifically addressed.

The lack of transparency itself must be considered within the law. Access Now recommends specific provisions to require reports, published at least once a year, which would indicate the extent of government hacking operations, including the number of users impacted, both foreign and domestic, the number of devices impacted, the length of the operations, and any unexpected consequences of the operation. We also recommend the requirement that a human rights impact assessment be conducted annually concerning hacking operations and technologies.

ii. Use Limitations

> *"Government hacking operations must be foreseeable by those who may be impacted by them. Therefore, authorization for government hacking must be specifically provided for by law, clearly written, and publicly available. The law should prohibit government hacking except in specific, limited circumstances. The information sought through government hacking should be defined with particularity in advance. Hacking should never be performed with either discriminatory purpose or effect."*
> *…*

[4] A Human Rights Response to Government Hacking at 22.
[5] http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.
[6] Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali at 2.

"Extraterritorial government hacking should not occur absent authorization under principles of dual criminality."[7]

We take positive note on the existence of a constitutional right in Italy to the inviolability to the digital domicile, embodied in Article 14. As personal digital devices hold more data about an individual, including primarily data that would have previously been stored physically within the home, the incorporation of this right is not only important, but it just makes good sense.

We appreciate the provision within the proposal that seeks to establish strict use limitations for these authorities. As Parliament continues to consider these use limitations, we encourage members to take into account the need for particularity and for provisions prohibiting any discriminatory use. This includes any use of tools to specifically or disproportionately target non-Italians. Not only would such targeting undermine human rights protections, but when targeting data of non-Italians stored abroad it would be contrary to protections under Mutual Legal Assistance Treaties (MLATs), long-established systems for obtaining cross-border access to data. MLATs were designed to ensure that law enforcement can receive access to data necessary for investigations that is stored outside of a country while respecting and maintaining the legal protection of the individual's legal framework.[8] Government hacking should not be allowed to act as an end-run around the systems in place.

Finally, any law must also generally prohibit government utilization of hacking tools to control public sentiment or cause damage to people, devices, or infrastructure.

iii. Integrity of Data Collected

Government hacking operations must never occur in perpetuity. Authorizations for government hacking must include a plan for concluding the operation. Government hacking operations must be narrowly designed to return only specific types of authorized information from specific targets and to not affect non-target users or broad categories of users. Protected Information returned outside of that for which hacking was necessary should be purged immediately.[9]

We strongly support the provisions in Civici e Innovatori's proposal intended to ensure integrity, authenticity, and immutability of data and devices impacted by government hacking operations.[10] This includes the establishment of an agency to approve hacking tools, documentation of all operations performed using those tools, the ability for targets to obtain that documentation and independently evaluate the process through which it was used, the creation of a national registry of hacking tools, and a requirement that the tool will not degrade security on a targeted device and that they will be un-installed at the end of an operation.

[7] A Human Rights Response to Government Hacking at 20; 22.
[8] *See* MLAT.info.
[9] A Human Rights Response to Government Hacking at 20.
[10] *See* Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali at 6.

We will go further into detail on individual provisions, but generally they should come with significant mandatory reporting so that the public can be made aware of their effectiveness and that officials in other governments can learn from the implementation of this proposal.

iv. Other Provisions

There are several other provisions in the proposal that we believe will help protect human rights. First, we are in favor of the provision that prohibits the use of contractors to employ hacking tools.[11] However, it is important that this limitation not extend to the use of independent oversight mechanisms, including auditing, to ensure that the tools are being deployed properly, not creating additional security vulnerabilities, and ensuring, as required, that collected data is adequately protected against unauthorized access.

As well as adding provisions to ensure independent oversight, we also encourage Civici e Innovatori to include mandatory retention limits on data collected through government hacking operations such that no data can be stored in perpetuity.

B. Specific Provisions

The unofficial english translation of the specific provisions that this section refers to are included in the appendix to the submission.

i. Article I

Access Now recognizes the positive steps in this Article to require approval of any government hacking operations, to limit those operations to only serious crimes, and to require notice be given to those impacted.

This section should be modified to specify that, to the greatest extent possible, all devices on which remote data capture is ordered should be located within Italy's jurisdiction and, if not, that officials must proceed through the Mutual Legal Assistance Treaty process. Further, while a prosecutor should commission the acquisition, an independent judge should have full authority to substantively review the application to ensure that it is meeting the legal standards and to approve or deny the application accordingly.

When another entity has control over data stored on an external hard drive, remote access should not be considered "absolutely essential for the continuation of investigations."[12] Instead, when data is stored on an external hard drive authorities should send a request either directly to the entity holding the data or via an MLAT request through another country.

[11] *See* http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf.
[12] *See* Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali at 9.

A presumption should be established that notice would be provided prior to the search there is a clear case for delay.

ii. Article II

The requirement that all hacking operations be taken out with respect for human dignity and privacy is commendable. To ensure that such respect is maintained in operations, the law should include mandatory public reporting requirements as well as provide for independent oversight and auditing. The law should also explicitly provide for limitations on access to the data collected pursuant to these operations, as well as provide for limitations on the scope of data that can be retained, and the amount of time that even that data may be kept should respect the general standards for data retention for investigations as established under the European Union's legal framework.[13]

iii. Article IV

Access Now supports the incorporation of the human rights standard of necessity into this proposal, and also the requirement that hacking only be used as a final resort. A new application should be filed for every device that officials seek to access and for every new type of collection sought to be conducted (e.g., video or audio). The number of applications submitted and approved should be publicly reported in separate categories for each type of collection.

iv. Article V

This Article establishes requirements for ensuring the integrity, authenticity, and immutability of data and devices impacted by government hacking operations. This goal is of paramount importance and Access Now commends Civici e Innovatori for its inclusion.

While Access Now supports each of the provisions in this Article, subject to the below comments, we would voice particular support for two provisions: the prohibition on adding or modifying data on a targeted device and the requirement to remove all computer tools or provide the information to do so after the operation has ended. While these provisions should also be accompanied by adequate transparency and accountability measures to ensure that they are complied with by all officials, they are essential to ensuring the goals of this Article are accomplished.

However, the need to ensure independent audits of operations and tools is necessary to ensuring that the tools have been properly and securely designed and that data impacted by

[13] *See* http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=624233.

the tools is secured from any unauthorized access. Judges should be provided with resources and empowered to hire staff with sufficient technical expertise to fully understand the scope of the hacking operations that they are being asked to approve.

While it is good practice to (securely) maintain a copy of collected data in order to facilitate access by auditors and impacted individuals, it should be subject to retention limits to ensure that no personal information is retained indefinitely. Finally, while it is positive to indicate that any information acquired in violation of the standards set out cannot be used, the provision should be clarified to indicate that the information can neither be used in investigations nor in prosecution, and that, subject to retention needed to provide notice to the target and for any subsequent legal challenge brought by that target for unlawful action by government officials, it should be quickly purged from any database.

v. Article VI

Similar to the prior Article, this Article seeks to establish rules, procedures, and systems to ensure technical soundness in the development and use of hacking tools and technologies. Access Now supports the goals of the different provisions in this Article, including the verification of programs which can ensure that parties involved in a case are confident about the capabilities of a hacking tool and the requirement that the use of hacking tools should be properly logged during investigations. These provisions will work together to increase the accountability of government hacking operations and ensure proper documentation is available for any internal or external reviews or audits.

However, this Article should clarify that source code should be written to ensure clarity, particularly in regard to the intelligence and consistent naming of program variables. Any tool for which the source code is overly difficult to read or understand should be rejected from the approved tools list. For any change in a tool's source code, the vendor should supply the change log along with user documentation and known bugs list for the present version.

Particularly promising in this Article are the requirements placed on officials following the installation of a hacking tool, namely that security measures that are lowered by the installation or use of the tool be restored as soon as possible and that removal of those tools should be implemented or at least facilitated following an investigation.

Together these requirements will likely ensure that devices targeted by hacking operations are not impacted long-term and can be returned to their original state. This is positive since devices may be re-sold or re-purposed and any state-induced vulnerabilities could increase future risk. However, this is also a lofty goal and the public would be well-served if officials were required to report annually on the implementation of these provisions, including the number of times tools were able to be successfully removed, the number of times individuals had to be provided with information on how to remove them personally, and the number of

times, if any, that the removal of hacking tools caused additional problems with devices or software.

Finally, Access Now supports the requirements to assure that evidence gathered during government hacking operations has not been tampered with, including through the creation of digital logs on the use of any hacking tool in an understandable format. However, the provision that requires that a party involved in an investigation must pay the vendor to prove the steps taken through the hacking tool creates an undue burden on individuals to prove their innocence. In cases where other evidence suggests that tampering may have occurred or where the provided data acquits the party involved than the cost should be waived or covered by the state officials.

vi. Article VIII

We caution Italy's use of increased penalties for the "criminal abuse" of hacking tools. While these provisions have been established to serve a legitimate goal, they could easily be expansively interpreted to criminalize necessary security research that uncovers critical vulnerabilities in software and services. Increased penalties for damaging critical infrastructure and national security system would deter security research on the most important systems making them more susceptible to unnoticed vulnerabilities. Moreover the language provides prosecutors broad leeway for increased penalties, for example, when damage to national security and critical infrastructure might be unintended or inconsequential or when when those systems are broadly defined.

III. Conclusion

Thank you for this opportunity to provide comments on this draft. We are appreciative of Civici e Innovatori's engagement on this important issue and incorporation of several human rights protections into the draft proposal. We would appreciate the continued opportunity to engage. If you have any questions about our submission or our report, please e-mail Amie Stepanovich at amie@accessnow.org.

Sincerely,

Amie Stepanovich
Global Policy Counsel

Lucie Krahulcova
EU Policy Association

Megan White
Congressional Affairs Intern

Appendix: Text of Relevant Provisions (unofficial English translation provided to Access Now)

Article I

"In organised crime cases of terrorism or Mafia kind, when it is not possible to distinguish between a business environment or personal life foreign to any criminal activity, the judge, at the request of Public Prosecutor, may order the observation of devices and remote data capture from a informations system or telematic system different to those relatively found in telephone or telematic traffic, only when there are serious indications of the offense and when the observation and remote capture are absolutely essential for the continuation of investigations. Each acquisition has to be authorised by the Public Prosecutor and validated by decree justified by the GIP."

"The authorisation decree referred to in Paragraph 1, must be notified to the person under investigation, other parties, and, if different, the owners and users of the devices within 40 days of the start of activities, or where there is reason to believe that the notification could derive serious injury to the investigation, the Judge, upon request of the prosecutor, may extend this period every 40 days and up to a maximum of 12 months with the action adequately justified."

Article II

"When the actual nature of the criminal organization does not present the pervasive connotations such as to hinder separation of illicit and ordinary private life, the court may deny or revoke authorization."

"The acquisition of data and information following the use of these programs or tools must be always carried out with respect for human dignity and personal and, as far as possible, respecting the modesty and privacy of the private sphere of those who are subjected."

Article IV

"'The planned operations'...can only be authorised if it is essential, with every other means for searching for proof becomes inadequate. In such cases the Judge must state the type of interception, if telematics, voice, messaging or other, and communications that are intended for interception."

Article V

"The programs or the tools used for the execution of operations must ensure, by the adoption of appropriate technical and procedural measures, that the data on the device cannot be tampered or modified, and that the collected data is consistent with the original data on the same device."

“The acquired computer data is stored with which to ensure the integrity, authenticity and immutability of data collected and their conformity to the originals. On expiry of the period specified in the decree of authorization, a copy of the data acquired during the activities is preserved at the offices or systems installed in the Prosecutor's Office.”

“The installation of programs or tools used must be authorized by the judge, by a justifying decree in which the devices are identified for which its installation and the reasons are detailed for why the installation is required on devices of subjects who are not suspects.”

“The installation is documented in a special report in stating the unique identification codes of Judicial operating police personnel, the name and version of the program and of the instruments used and their manufacturers. In the record of the operations, observation, remote acquisition and interception are also indicated, even summarily, the type of communications and data intercepted or acquired remotely and the technical measures taken to ensure their preservation and integrity.”

“The public prosecutor may delegate the task only to the judicial police, that cannot make use of auxiliaries.”

“On completion of the program or the computer tools used it must be removed from the device on which they were installed and this operation’s minutes shall be taken; in case the removal is not possible, technical information necessary for removal must be provided to the user so they can independently.”

“The programs and tools used in accordance with paragraphs above shall meet the requirements established by regulation of the Minister of Justice, in consultation with the Minister of the Interior and of opinion complying with the Authority for the Protection of Personal Data.”

“The information and data acquired in violation of the provisions of Articles 267, 268 and this Article cannot be used.”

Article VI

“This decree, to be updated at least every three years, establishes the requirements that the technical programs or tools must meet to ensure that their installation and activation for the observation and remote capture data does not change the data itself or other features of the host device; the manner in which discipline should be ensured for compliance of the program used to the stated requirements as well as the relative procedures for using and updating and, finally, includes the specific detail about using and updating the program, on the basis of the following guiding criteria:

“A. Establishment of a type-approval entrusted to the Institute of Superior Communications and Information Technology (ISCOM), of computer programs and tools that

can be used under Article 266-bis, 266-ter and 254-ter of the c.p.p.; The approval shall be repeated at least every 12 months to ensure the validity of all editions of intermediate captators released as updates for already approved editions.

"B. Introducing a source codes filing requirement at an institution to be determined by such in a procedure to ensure, a posteriori, repeatability independent of a specific certification process edition of the tool or program, reproducing the exact copy the program used in the process of investigation from its source codes, and all its intermediary editions instantiated and/or installed, if the identification footprint is different. The deposit of the codes sources must be made for each software edition released by the manufacturers at least every 12 months. The deposit of source codes must be made for every single software edition made by its manufacturers at least every 12 months.

"C. Introduction of a guarantee of traceability of the tool or program under use, such as to enable the parties to validate the legitimacy of introducing an appropriate database, a National Registry of informatic captators, which collects in real time and with guarantee of integrity of data as well as temporal validity, all the digital fingerprints of all the editions of captators that are type-approved issued by manufacturers and installed on targeted devices for investigation; The registry will be operated by the institution of approval at the disposition of the public security forces, information services and the representatives of the parties directly affected by the intrusion computer. Requests for information, possible only by the lawyers defending the suspects who were being followed up through captators, will not have any burden for applicants and must be completed within 30 days of the request.

"D. Expectation of a registration requirement for all operations carried out by the instrument or computer program, its installation until its removal, fully made arrangement of the parts of the case file as an attachment, so as to ensure the authenticity and integrity of the data;

"E. Prevision of a ban, for the stated program or tool that would lead to a lowering of the current system's security or device on which its used. There is an exception exclusively for any installation phases that require a temporary lowering of security level of the system or the device, which would then have to be brought back to its original condition at the end of the installation procedure, whether successful or not.

"F. Prevision of an obligation, by the end of use of the stated tools and programs, to provide for their removal and, in case the removal is not possible, technical information necessary for removal must be provided to the user so they can independently.

"G. Introduction of a requirement for making available by the manufacturer, publicly and free of charge, the software tools necessary for the analysis of the attachments on the case file referred to in point D, inclusive of related technical documentation and data format specification. These tools must enable the parties to check in independently of compliance with integrity requirements as well as the completeness of the attachments of the case file of which at point D, or validate that this includes the registration of all phases of operation of the captator, from the specific instance generation, to all actions carried out until its uninstallation.

"H. Introduction of a system which allows the parties to request and perform verifications in an independent manner the process of type-approval. The procedure of verification provided by the manufacturer must ensure the, a posteriori, repeatability of the

approval process of a specific edition of the program or tool, reproducing the exact copy of the program used in the investigation stage starting from its source code, and all its instantiated intermediate editions and/or installed editions. The manufacturer must provide as a paid service, on requests of the parties involved in a case that sees the use of a captator from these certified, a provision of technical personnel and/or documentation to explain the operation of the system. The tariff that the manufacturer can propose may not exceed the average price charged by the technical consultants in comparison to prosecutors, for advice concerning c.d computer forensics."

Article VIII

"If the intrusion to computer system is also committed using observation tools and remote capture, producing damage to the national security and of critical infrastructure of the penalties country increased from a third to half

…

"[it is an aggravated crime] if the act is committed in order to illegally process personal data sensitive or judicial, or at least if following these computer intrusion data are disseminated illegally by any other means of communication."