A HUMAN RIGHTS RESPONSE TO GOVERNMENT HACKING

Recently we have seen several high-profile examples of governments hacking into consumer devices or accounts for law enforcement or national security purposes. Access Now released a report where we consider government hacking activity from the perspective of international human rights and conclude that based upon its serious interference with the rights to privacy, free expression, and due process, there should be **a presumptive prohibition on all government hacking**.

There has yet to be an international public conversation on the scope, impact, or human rights safeguards for government hacking. The public requires **more transparency** regarding how governments decide to employ hacking and how and when hacking activity has had unanticipated impacts. Finally, we propose **Ten Human Rights Safeguards for Government Hacking** in pursuit of surveillance or intelligence gathering. The full report is available at:
www.accessnow.org/GovernmentHackingDoc

WHAT IS GOVERNMENT HACKING?

We define 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 the device, data, or service or who is ultimately affected by the manipulation.

We consider government hacking in three categories based on the broad goal to be achieved: to control a message, to cause damage, or to conduct surveillance.

1	2	3
Messaging control	**Causing damage**	**Commission of surveillance or intelligence gathering**
Hacking to control the message seen or heard, specifically by a particular target audience.	Hacking to cause some degree of harm to one of any number of target entities.	Hacking to compromise the target in order to get information, particularly on an on-going basis.

HOW DOES GOVERNMENT HACKING IMPLICATE HUMAN RIGHTS?

All government hacking substantially interferes with human rights, including the right to privacy and freedom of expression. While in many ways this interference may be similar to more traditional government activity, the nature of hacking creates new threats to human rights that are greater in both scale and scope. Hacking can provide access to protected information, both stored or in

transit, or even while it is being created or drafted. Exploits used in operations can act unpredictably, damaging hardware or software or infecting non-targets and compromising their information. Even when a particular hack is narrowly designed, it can have unexpected and unforeseen impact.

Based on analysis of human rights law, we conclude that there must be a presumptive prohibition on all government hacking. In addition, we reason that more information about the history and the extent of government hacking is necessary to determine the full ramifications of the activity.

In the first two categories — messaging control and causing damage — we determine that this presumption cannot be overcome. However, we find that, with robust protections, it may be possible, though still not necessarily advisable, for the government to overcome the presumptive prohibition in the third category, government hacking for surveillance or intelligence gathering. We note that the circumstances under which it could be overcome are both limited and exceptional.

In the context of government hacking for surveillance, Access Now identifies Ten Human Rights Safeguards for Government Hacking, including vulnerability disclosure and oversight, that **must** both be implemented and complied with to meet that standard. Absent government compliance with all ten safeguards, the presumptive prohibition on hacking remains. In addition, the high threat that government hacking poses to other interests, defined in greater detail in our report, may (and probably should) necessitate additional limitations and prohibitions.

Government hacking threatens human rights embodied in international documents.

Universal Declaration of Human Rights (relevant provisions):	
Article 10:	"Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him."
Article 12:	"No one shall be subjected to arbitrary interference with his privacy, family, home[,] or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacksattacks."
Article 17:	"(1) Everyone has the right to own property alone as well as in association with others. (2) No one shall be arbitrarily deprived of his property."
Article 18:	"Everyone has the right to freedom of thought, conscience[,] and religion..."
Article 19:	"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive[,] and impart information and ideas through any media and regardless of frontiers."
Article 20:	"(1) Everyone has the right to freedom of peaceful assembly and association. (2) No one may be compelled to belong to an association."

APPENDIX: TEN HUMAN RIGHTS SAFEGUARDS FOR GOVERNMENT HACKING

There should be a presumptive prohibition on all government hacking. In any instance where government hacking is for purposes of surveillance or intelligence-gathering, the following ten safeguards must all be in place and actually complied with in order for a government to successfully rebut that presumption. Government hacking for the purposes of messaging control or causing damage cannot overcome this presumption.

1. Government hacking must be provided for by law, which is both clearly written and publicly available and which specifies the narrow circumstances in which it could be authorized. Government hacking must never occur with either a discriminatory purpose or effect;
2. Government actors must be able to clearly explain why hacking is the least invasive means for getting Protected Information in any case where it is to be authorized and must connect that necessity back to one of the statutory purposes provided. The necessity should be demonstrated for every type of Protected Information that is sought, which must be identified, and every user (and device) targeted. Indiscriminate, or mass, hacking must be prohibited;
3. 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;
4. Applications for government hacking must be sufficiently detailed and approved by a competent judicial authority who is legally and practically independent from the entity requesting the authorization and who has access to sufficient technical expertise to understand the full nature of the application and any likely collateral damage that may result. Hacking should never occur prior to authorization;
5. Government hacking must always provide actual notice to the target of the operation and, when practicable, also to all owners of devices or networks directly impacted by the tool or technique;
6. 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;
7. Government hacking operations must never compel private entities to engage in activity that impacts their own products and services with the intention of undermining digital security;
8. If a government hacking operation exceeds the scope of its authorization, the agency in charge of the authorization should report back to the judicial authority the extent and reason;
9. Extraterritorial government hacking should not occur absent authorization under principles of dual criminality;
10. Agencies conducting government hacking should not stock vulnerabilities and, instead, should disclose vulnerabilities either discovered or purchased unless circumstances weigh heavily against disclosure. Governments should release reports at least annually on the acquisition and disclosure of vulnerabilities.

In addition to these safeguards, which represent only what is necessary from a human rights perspective, the judicial authority authorizing hacking activity must consider the entire range of potential harm that could be caused by the operation, particularly the potential harm to cybersecurity as well as incidental harms that could be caused to other users or generally to any segment of the population.