NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

HAUT-COMMISSARIAT AUX DROITS DE L'HOMME • OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9000 / 9278 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org; freedex@ohchr.org

2 March 2016

Re: In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203
ED No. CM 16-10 (SP)

The Hon. Sheri Pym,

I am the United Nations (UN) Special Rapporteur on the protection and promotion of the freedom of opinion and expression, appointed in June 2014 by the UN Human Rights Council, the central human rights body in the UN system. In this capacity, I monitor freedom of expression issues worldwide, including individual rights in a digital age, the protection and safety of the media, and the rights enjoyed by members of vulnerable communities, activists, political dissenters, and many others. I am also a Clinical Professor of Law at UC Irvine School of Law.

In my position as Special Rapporteur, I have had the opportunity to study how secure communications -- in particular through such measures as encryption and anonymity online -- advance freedom of opinion and expression. Last June, as required by my mandate, I presented to the Human Rights Council a report on human rights and secure communications that analyzed how encryption advances freedom of expression online and identified the human rights framework applicable to restrictions on such freedom of expression (UN Doc. A/HRC/29/32; 22 May 2015). My analysis and recommendations rested upon the International Covenant on Civil and Political Rights (ICCPR), the central treaty in international human rights law and one to which the United States, which ratified the ICCPR in 1992, and 168 other countries are bound.

Because of the direct relevance to the case before you, I respectfully wish to share with you a copy of this report, which is attached (pdf format).

I believe that the ICCPR bears directly upon the subject matter before you. While a number of provisions may apply, I wish to highlight one. Article 19 of the ICCPR provides:

"1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of

The Honorable Magistrate Judge Sheri Pym
United States District Court
Central District of California
Riverside, California
Email: SP_chambers@cacd.uscourts.gov; Kimberly_Carter@cacd.uscourts.gov

frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (*ordre public*), or of public health or morals."

My report argued that secure communications are fundamental to the exercise of freedom of opinion and expression in the digital age, permitting the maintenance of opinions without interference and securing the right to seek, receive, and impart information and ideas. Encryption allows for zones of privacy that enable all sorts of expression. From the report:

"11. … an open and secure Internet should be counted among the leading prerequisites for the enjoyment of the freedom of expression today. But it is constantly under threat, a space — not unlike the physical world — in which criminal enterprise, targeted repression and mass data collection also exist. It is thus critical that individuals find ways to secure themselves online, that Governments provide such safety in law and policy and that corporate actors design, develop and market secure-by-default products and services. None of these imperatives is new. Early in the digital age, Governments recognized the essential role played by encryption in securing the global economy, using or encouraging its use to secure Government-issued identity numbers, credit card and banking information, business proprietary documents and investigations into online crime itself.

12. Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression."

To the extent that the subject order leads to vulnerabilities in secure communications, compromises in the ability of individuals worldwide to fight and evade the consequences of censorship, and precedent that could be deployed on other platforms moving forward, I believe that the implications for freedom of expression are potentially quite serious.

Article 19(3) permits restrictions where provided by law and are necessary and proportionate to protect, among other things, national security and public order. Law enforcement and national security officials raise legitimate concerns about the barriers posed by encrypted communications, whatever the device. My report noted the following:

> "13. The 'dark' side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism."

The government in this case enjoys a clearly legitimate interest when it comes to public order and national security, but the subject order deserves scrutiny under Article 19(3). First, one question is whether the order is based on authority that would be considered "provided by law." The All Writs Act, a catch-all provision enacted in an era far pre-dating the existence of digital communications, may not satisfy this condition. Assuming, however, that the All Writs Act is sufficient to meet that standard, Article 19 then requires determining whether the restriction is "necessary… for the protection of national security or of public order". Given that the Government has multiple, alternative technical and operational measures to conduct this investigation, it is unclear that the Government's motion to compel Apple to create software to enable access to this iPhone is necessary for this particular investigation.

The requirement of necessity under Article 19 includes within it the concept of proportionality (see para 35 of the report for my discussion with an array of sources; the Human Rights Committee, the monitoring body of the ICCPR, emphasized this point in its interpretive General Comment 34, starting at para 22; and governments by and large agree with this understanding of necessity under Article 19). My concern is that the subject order implicates the security, and thus the freedom of expression, of unknown but likely vast numbers of people, those who rely on secure communications for the reasons identified above and explicated in more detail in the report. This is fundamentally a problem of technology, one where compromising security for one and only one time and purpose seems exceedingly difficult if not impossible. Again from the report, "States must show, publicly and transparently, that other less intrusive means are unavailable or have failed and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim." (para 43) It is not clear that the Government has tried other means short of compelling Apple's code-writing in this case, such as enlisting the technical expertise of other agencies to access this particular phone.

I respectfully ask that this letter and the attached report be accepted into the record of this case and placed on the docket. Thank you very much for your consideration.

Please accept the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the
right to freedom of opinion and expression

cc:

Permanent Mission of the United States of America to the United Nations Office and other international organizations in Geneva, H.E. Ms. Pamela K. Hamamoto, Ambassador and Permanent Representative, and David Sullivan, Attaché (SullivanDB@state.gov)

United States Department of Justice, Tracy Wilkison (tracy.wilkison@usdoj.gov)

Gibson Dunn (NHanna@gibsondunn.com; TBoutrous@gibsondunn.com; evandevelde@gibsondunn.com)

ZwillGen PLLC (marc@zwillgen.com; jeff@zwillgen.com)