Speaking Notes

My name is Cara Zwibel and I am a lawyer and program director with the Canadian Civil Liberties Association (CCLA). The CCLA is a national, non-profit, non-partisan and non-governmental organization supported by thousands of Canadians from all walks of life. This year CCLA celebrates 50 years of working to advance these goals. In our role as a defender of fundamental rights, including freedom of expression, the right to privacy and the right to be free from unreasonable state intrusion, I am grateful for the opportunity to appear before the Committee and raise some of our concerns about aspects of Bill C-13.

My comments today will be focused on two main areas. First, the creation of the new offence of the non-consensual distribution of intimate images. We believe that the new offence is overly broad and that it will open the door to capturing lawful activity in a way that may unreasonably violate freedom of expression.

Second, I want to address the new investigative powers included in the Bill. Most of Bill C-13 is dedicated to increasing police investigative powers. To the extent that some gaps have been identified in the ability of investigators to deal with online crime, such measures are appropriate. However, in our view the provisions of C-13 do not strike an appropriate balance between investigative necessity and personal privacy rights. They authorize unreasonable intrusions by the state into
the personal lives of Canadians. CCLA cannot support the Bill without substantial amendments to the investigative powers provisions.

A) The Non-Consensual Distribution of Intimate Images

I am going to begin with the new offence of non-consensual distribution of intimate images, and in starting on this point I want to acknowledge that cyberbullying is a concern to many Canadians and, indeed, CCLA shares the view that local, provincial and federal governments have a role to play in addressing this ongoing challenge.

There are certainly real harms and a great deal of embarrassment that may flow from the distribution of intimate images, but the creation of a new criminal offence is a blunt instrument. Using it to address the cyberbullying problem may lead to criminalizing the victims just as much as the perpetrators.

At the most basic and fundamental level, this new offence criminalizes expression. Even expression that is hurtful, embarrassing or deeply offensive is protected by the Canadian Charter of Rights and Freedoms and may only be limited in a manner that is both reasonable and demonstrably justified in a free and democratic society. Restriction on expression should be narrowly tailored to achieve their intended goals.

In our view, the proposed offence is broadly written and, as a result, limits freedom of expression in a manner that is unreasonable on a number of counts:

First, the offence does not require malicious intent. In light of the ubiquity of intimate images that are floating around in cyberspace, the absence of a malicious intent requirement means that individuals could be held criminally responsible simply for posting, sharing or sending an intimate image that is already “out there” online (perhaps first posted by the individual depicted) and that depicts someone they don’t even know.
Second, the definition of what constitutes an “intimate image” is too broad and its use of the “reasonable expectation of privacy” standard will pose difficult challenges to the courts charged with interpreting and applying the law. The concept of a reasonable expectation of privacy, used to give meaning to the right to be free from unreasonable search and seizure pursuant to s. 8 of the Charter, is a complex one that has been the subject of much judicial discussion and consideration. The section 8 Charter jurisprudence addresses the privacy interests that individuals have as against the state. The proposed offence, however, deals more with the expectations of privacy that people have vis-à-vis other individuals and society at large. This concept will be difficult to interpret and apply when the images at issue were not created by the accused and could have emanated from any number of sources.

Third, CCLA is concerned about the orders that may be imposed on individuals convicted of the new offence, particularly orders that prohibit the offender from using the Internet or other digital network. Such a condition, which may be imposed without terms that limit its scope or duration, is draconian. Prohibiting individuals from accessing the Internet may effectively isolate them from friends and family, significantly hamper their ability to access information and communicate with the world around them, and negatively impact the employment prospects and educational opportunities for an offender. CCLA believes that this section must be significantly narrowed and include a maximum prohibition period of one year.

As currently drafted, the new offence created by Bill C-13 casts too wide a net and the recklessness standard that it employs is much too low for an offence that criminalizes such a broad range of expression.

B) Investigative Powers
I would like to move now to discuss the new investigative powers contained in the Bill as these give rise to a number of very serious concerns, particularly in light of information that has recently emerged about the extent to which government institutions are already requesting and receiving personal information from telecommunications service providers and internet service providers, without prior judicial authorization and without the knowledge or consent of their customers.

i) **Immunity Provision – s. 487.0195**

CCLA is pleased that many of the more intrusive provisions from prior incarnations of lawful access legislation have been dropped, but we remain concerned about several aspects in the Bill and, in particular, s. 487.0195(1) and (2) [contained in clause 20 of the Bill]. This section purports to grant immunity from any criminal or civil liability to any person who preserves data or provides a document to law enforcement where there is no legal prohibition on doing so. On its face, this provision appears to be redundant – it simply states that an individual will not incur liability for doing something that is not prohibited by law. The Minister has made statements indicating that this section doesn’t do anything new, and is simply there for greater clarity. I have also followed the Committee’s hearings on this issue and understand that many Committee members continue to believe this provision is totally innocuous. I have to take issue with this characterization and want to caution the Committee against allowing this provision to go forward.

Contrary to the Minister’s statements, the immunity provision could have far-reaching implications and is deeply problematic. In particular, this provision seeks to exploit some of the confusion and ambiguity around the legality of disclosing personal information to law enforcement without a warrant. It also seeks to take advantage of the ambiguity in existing privacy legislation and the evolving nature of what
constitutes a reasonable expectation of privacy in light of increasingly advanced and privacy-invasive technologies. For example, currently the federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), requires that corporations that collect personal information in the course of their commercial activities not disclose that information without the knowledge and consent of the individual. There are a number of significant exceptions to this rule, many of which are drafted in extremely broad terms and include providing information to government agencies including law enforcement officials in a wide variety of circumstances. There remains differing interpretations on the permissible scope of these exceptions, and, in light of this ambiguity, corporations may take a more cautious and privacy-protective approach to customer data out of fear of liability. A cautious approach is certainly warranted given that law enforcement has the expertise and ability necessary to seek out a search warrant. The immunity provision is a blatant attempt to incentivize private corporations to cooperate with law enforcement even when doing so poses a genuine risk to customer privacy and may not serve any compelling state objective. This provision should be moved from the Bill.

**ii) Reasonable suspicion**

A number of the new investigative powers included in Bill C-13 allow for the preservation of data and the production of documents based on the low standard of “reasonable grounds to suspect”. This standard has been found, by our courts, to be appropriate in certain contexts where the reasonable expectation of privacy is relatively low. Bill C-13, however, uses this standard to authorize warrants for transmission and tracking data.¹ Contrary to statements made by some that this is simply

---

¹ In particular, see proposed ss. 487.015, 487.016, 487.017 of the *Criminal Code*, s. 20 of Bill C-13.
“phone book” information, this kind of data can be highly invasive and provide a detailed and intimate profile of an individual. Indeed, many studies have suggested that, in some cases, the information that can be gleaned from this kind of data is greater than actually monitoring the content of communications. CCLA believes that warrants for this kind of information should only be granted on the stricter standard of reasonable grounds to believe. In addition, the provisions establishing the rules around production orders for both tracking and transmission data appear to require only that the data will assist in an investigation. Given the invasive nature of these kinds of orders, a higher standard is required. A standard of investigative necessity or a requirement that the data will afford evidence of an offence, would be more appropriate.

I would also like to point out some implications that result from changes to the definition of a ‘tracking device’ and a ‘transmission recorder’. The definitions have been changed to include software. This means that provisions authorizing the use of a tracking device or transmission recorder effectively allow for the installation of malware. Police are being given the power to remotely hack into computers, mobile devices, or cars in order to track location and/or record metadata. This is extremely invasive and should certainly not be subject to the lower standard of reasonable grounds to suspect. This is a very big shift and certainly deserves more careful study.

iii) Public officer

On the subject of new definitions, CCLA is also concerned that the Bill includes a change to the definition of a “public officer” who, along with a peace officer, may take steps to obtain all kinds of orders, including

---

production orders related to tracking and transmission data. The *Criminal Code* currently defines “public officer” by way of a closed list of individuals, while Bill C-13 would amend the definition to include “a public officer who is appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament”. This is a substantial broadening of the existing list. There has been no compelling evidence provided to demonstrate why the current scheme doesn’t work and why a larger number of individuals should be able to seek these invasive orders from a judge or justice of the peace. CCLA believes this proposed change should be abandoned.

**iv) Prohibitions on disclosure**

Finally, I would like to address concerns around the total absence of transparency and accountability mechanisms related to the new police powers created by C-13. The new production order powers may result in the disclosure of significant amounts of personal information to law enforcement and a range of others (in light of the expanded definition of ‘public officer’). The Bill includes a provision for keeping confidential the very existence of these orders throughout their duration, subject to judicial authorization. CCLA appreciates that investigative integrity may require that these orders remain confidential for some time. However, it is unreasonable to keep this information confidential indefinitely. Moreover, mandatory proactive disclosure of the existence of these orders should be added into the Bill to require disclosure once confidentiality is no longer required. Such a system is already in place with respect to wiretaps, and given the sensitivity and nature of information captured by some of the new production orders, similar safeguards are required.
C) Conclusion

To conclude, Bill C-13 makes substantial and complex changes to the Criminal Code. We believe many of these changes are problematic and may violate constitutional norms by allowing intrusion by the state into the personal lives of individuals absent compelling objectives and stringent standards. The absence of accountability and transparency mechanisms is particularly troubling since as police powers are increased, concomitant changes must be made to accountability systems.