



DEPARTMENT OF JUSTICE

Transmission Data: Considerations for Criminal Law Policy

Department of Justice, Canada
February 2005





Main Challenges

- First challenge: in modernizing definition must address contemporary telephony but must extend beyond to also deal with Internet “traffic data” but avoiding the pitfalls that threaten “technology-neutral language”
- Second: in constructing definition of “transmission data” some individuals have argued (sometimes following lead of legislative provisions in some countries) that such data “should not include the contents of any communication”
- Third: at a practical level, there are circumstances (“header information” in some packets; post-call cut-through digits in telephony) where “content” is apparently not excluded





The perils of “content”

- “Content” is not a helpful term: in those cases where it has been used, it has not been defined
 - Simply attempting to exclude “content” as such from transmission data is an over-simplification and does not provide a solution
 - Reasonable expectation of privacy has been defined through the courts; information attracting a reasonable expectation in accordance with appropriate threshold is the object of exclusion
 - Challenge: re-conceptualize problem to address *Charter* considerations but avoid unnecessary pitfalls of “content”
-



information attracting
reasonable expectation of privacy

- Core biographical information
- Lifestyle information
- personal information

“Content”
(undefined term)

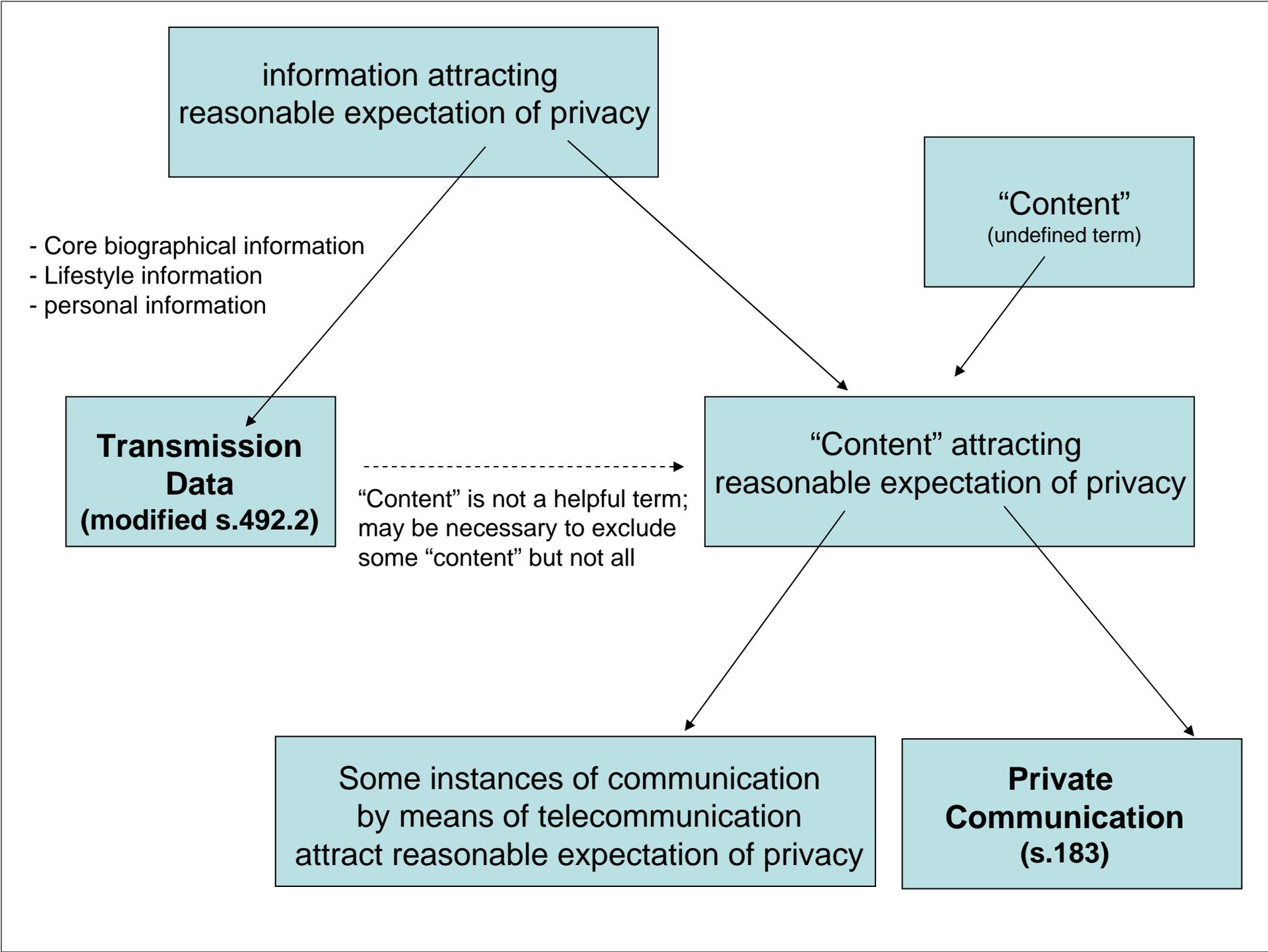
**Transmission
Data
(modified s.492.2)**

----->
“Content” is not a helpful term;
may be necessary to exclude
some “content” but not all

“Content” attracting
reasonable expectation of privacy

Some instances of communication
by means of telecommunication
attract reasonable expectation of privacy

**Private
Communication
(s.183)**





Acquiring what is needed

- **“transmission data”** means data
- relating to the telecommunications functions of dialling, routing, addressing or signalling
- that identifies or purports to identify
- the origin, type, direction, date, time, duration, size, destination or termination
- of a telecommunication
- generated or received by means of a telecommunications facility.



But only what is needed, no more

- **“transmission data”** means data
- relating to the telecommunications functions of dialling, routing, addressing or signalling
- that identifies or purports to identify
- the origin, type, direction, date, time, duration, size, destination or termination
- of a telecommunication
- generated or received by means of a telecommunications facility.



Transmission Data

- The argument is that core biographical information or content that attracts a reasonable expectation of privacy is not “data relating to the **telecommunications functions** of dialling, routing, addressing or signalling ”



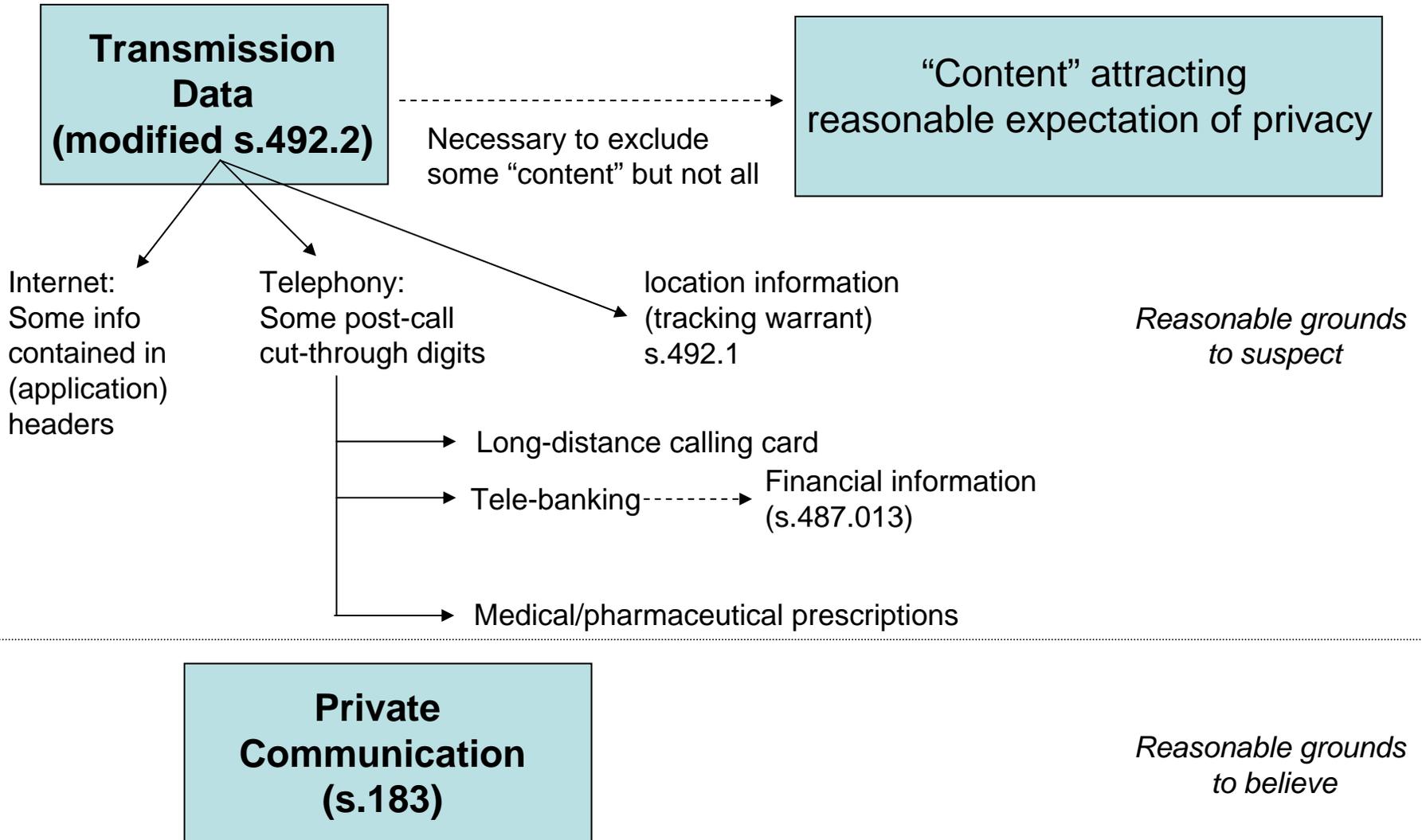


What is necessary for LEAs

- Data that identifies or purports to identify
 - the origin, type, direction, date, time, duration, size, destination or termination
 - of a telecommunication
- Are the attributes sufficient to capture all that is needed?
 - location is can be a distinct concept in this context and may be available in different respects depending on the technology

Information attracting reasonable expectation of privacy

- Core biographical information
- Lifestyle information
- personal information





Post-call Cut-through Digits

- Situation is not simple
- Some post-call cut-through digits fit within definition of transmission data
- Some post-call cut-through digits fall outside definition of transmission data but such information is already permissible at the same threshold (reasonable grounds to suspect) under another order (s.492.1 or s.487.013)
- Some post-call cut-through digits fall outside definition of transmission data and do not seem to correspond to any existing order at this threshold: how should these be addressed?



Issues in Practice

- Although some information is already permissible at the same threshold (reasonable grounds to suspect) under another order (s.492.1 or s.487.013), would an LEA request multiple orders from a judge?
- Although the disclosure or acquisition of such information is permissible at this threshold, is there a problem with the availability of a wide set of such information even if backed by multiple orders – I.e., although each is *Charter* compliant in isolation, was it envisaged that they would be conglomerated?





Header and Log Information

- Some header info and some log info should be disclosed at threshold of reasonable grounds to suspect
- Technical considerations: different kinds of headers – different info at different layers of the Internet protocol stack
 - Concerns arise with headers at the “application layer” rather than the lower layers of the protocol stack (“transport layer” for TCP or UDP headers; “network layer” for IP or ICMP headers; “data link layer” for frame headers)
- Concerns arise with information in some logs
 - eg. “GET page” entries in a Web log as opposed to network access information typically in a RADIUS log
- Possible solution: filtering



Contact

- For written submissions please contact:

Christopher Blain
Criminal Law Policy Section
Justice Canada
East Memorial Building, Room 5016
284 Wellington Street
Ottawa, Ontario K1A 0H8

Email: christopher.blain@justice.gc.ca
Tel: (613) 957-4688
Fax: (613) 941-9310