Law Enforcement Access to Subscriber Data in Canada
Backgrounder

Tamir Israel, Staff Lawyer, CIPPIC
March 3, 2017

1. What is, if at all, the law on the requirements for law enforcement's access to subscriber identity information?

The answer to this depends on context.

Canada's *Criminal Code*, recognizes a production power by which law enforcement can seek a production order compelling a financial institution similar to a bank to disclose basic account information. A court will only do so if law enforcement can demonstrate reasonable grounds to suspect an offence has been or will be committed and that the data sought will assist in an investigation of that offence. (section 487.018, *Criminal Code*, RSC 1985, c C-46). Law enforcement can compel any company to provide them with any and all customer data, including subscriber data, by means of a general production order. To obtain a general production order (*Criminal Code*, section 487.014), law enforcement must establish to a court the existence of reasonable grounds to believe a crime has or will be committed and that the data sought will afford evidence respecting said offence. Under Canadian law, 'reasonable grounds to believe' is a more demanding and rigorous standard than 'reasonable grounds to suspect'.

There have been a number of historical attempts to legislate a specific 'subscriber information' power that would permit law enforcement to compel service providers to disclose communications-related subscriber data upon demand. (Some of these are summarized in [1]). These past proposals employed an administrative authorization regime (meaning that law enforcement agents would generate the demands without any prior authorization from an objective decision-maker such as a court) and indiscriminate in nature (requiring a nexus to a law enforcement objective as a pre-requisite to their issuance, but no reasonable grounds that the subscriber information will assist in an investigation). To date, no such attempt has been successful, with past governments concluding that the indiscriminate access to communications-related subscriber data amounts to a disproportionate impact on privacy rights.

Some types of subscriber data may be obtainable by law enforcement on a voluntary basis, upon request. That is, in some contexts, law enforcement are permitted to ask organizations to provide subscriber data voluntarily, upon receipt of an informal request from law enforcement and without the need for a court order. The *Personal Information Protection and Electronic Documents Act* (PIPEDA), [2] Canada's federal private sector data protection regime, allows private companies to share customer data without customer consent where law enforcement can present 'lawful authority' (paragraph 7(3)(c.1). Historically, most Canadian communications access providers participated in a program by which subscriber data was voluntarily provided to law enforcement on request in situations purportedly related to child exploitation investigations. (The program is described in *R v Ward* [3]). Canadian communications access providers would voluntarily identify customers in other contexts not involving child exploitation on a case-by-case basis. Where voluntary disclosure by service providers was not forthcoming, law enforcement would rely on the general production power described above.

In 2014, the Supreme Court of Canada issued a decision (*R v Spencer*) [4] recognizing the importance of online anonymity as a constitutional value protected under section 8 of the Canadian *Charter of rights and freedoms*, which prohibits unreasonable search and seizure by the state. *Spencer* specifically held that individuals may reasonably expect that the state will not seek to identify their otherwise anonymous Internet browsing activity by asking their service provider to voluntarily identify them. In doing so, *Spencer* explicitly rejected the notion that communications service provider's subscriber data does not attract

constitutional privacy protection when obtained by the state for the purpose of identifying otherwise anonymous online activity:

> ... divergent views were reflected in the decisions of the Saskatchewan courts. The trial judge adopted the Crown's view that what the police sought and obtained was simply generic information that does not touch on the core of Mr. Spencer's biographical information. Ottenbreit J.A. in the Court of Appeal was of largely the same view. For him, the information sought by the police in this case simply established the identity of the contractual user of the IP address. The fact that this information might eventually reveal a good deal about the activity of identifiable individuals on the Internet was, for him, "neither here nor there" ... In contrast to this approach, Caldwell J.A. (Cameron J.A. concurring on this point) held that in characterizing the subject matter of the alleged search, it is important to look beyond the "mundane" subscriber information such as name and address (para. 22). The potential of that information to reveal intimate details of the lifestyle and personal choices of the individual must also be considered: see also *Trapp*, *per* Cameron J.A., at paras. 33-37.
>
> ...
>
> Applying this approach to the case at hand, I substantially agree with the conclusion reached by Cameron J.A. in *Trapp* and adopted by Caldwell J.A. in this case. The subject matter of the search was not simply a name and address of someone in a contractual relationship with Shaw. Rather, it was the identity of an Internet subscriber which corresponded to particular Internet usage. ... I conclude therefore that the police request to Shaw for subscriber information corresponding to specifically observed, anonymous Internet activity engages a high level of informational privacy.
>
> *R v Spencer*, 2014 SCC 43, http://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html

The *Spencer* decision also clarified that a service provider can only rely on paragraph 7(3)(c.1) of PIPEDA in order to disclose customer information on the basis of 'lawful authority' alone (that is, in the absence of a court order, a legislated administrative power compelling disclosure on demand, or consent from the affected customer) where the data sought is not protected by the section 8 of the *Charter*. As above, subscriber information sought for the purpose of identifying anonymous Internet activity is protected by section 8 because of its capacity for revealing details of private life. Prior to *Spencer*, it had been argued that any law enforcement officer acting within her the scope of her policing duties possessed the requisite 'lawful authority' to qualify for the exception in paragraph 7(3)(c.1).

Since the *Spencer* decision, the general production power described above has become the primary means for obtaining Internet-related subscriber data. This shift has been accompanied by renewed calls from Canadian law enforcement agencies to legislate a subscriber data power, and the federal Government is currently consulting on this question. Incomplete data is available on the scope of Canadian law enforcement access to subscriber data. Some data obtained by means of right to information demands may be indicative of the frequency of such requests, with pre- and post- *Spencer* comparisons [citations omitted]:

> ... since the introduction of the general production power, law enforcement have consistently and successfully relied upon such orders to obtain subscriber identification data from telecommunications companies in large volumes. Halifax Regional Police, for example, compelled production of telecommunications subscriber identification data approximately 4,507 times while only relying on voluntary disclosure by service providers 2,354 in the largely pre-Spencer period spanning January 2011 - December 2014. During the same period, the Vancouver Police Department obtained 25,189 production orders for subscriber identification data while relying on voluntary disclosure only 13,407 times. The general production power therefore enjoys a long track record of success in many investigative contexts. Indeed, past iterations of this justification exercise have similarly struggled to demonstrate any actual shortcomings in the existing framework, with internal law enforcement

> emails demonstrating an inability to find "sufficient quantity of credible examples" in support of unfettered access to subscriber identification data. [Data obtained by Dr Christopher Parsons by means of Provincial right to information regimes and on record with the author. Halifax Regional Police Dataset. Vancouver Police Department Dataset.]
>
> https://citizenlab.org/wp-content/uploads/2016/10/20161005-CNSCI-RevisitingAnonymityYetAgain.pdf

Transparency reports issued by some telecommunications providers suggest that subscriber information may still be provided voluntarily in support of exigent circumstance 9-1-1 calls. (see TELUS [5], Rogers [6])

Subscriber data may remain available to law enforcement upon request where other entities (such as electricity companies) voluntary comply and where the data sought will not have the effect of revealing private activities. (See *R v Plant*, [1993] 3 SCR 281:

> "The United States Supreme Court has limited application of the Fourth Amendment (the right against unreasonable search and seizure) protection afforded by the United States Constitution to situations in which the information sought by state authorities is personal and confidential in nature: *United States v Miller*, 425 US 435 (1976). ... While I do not wish to be taken as adopting the position that commercial records such as cancelled cheques are not subject to s. 8 protection, I do agree with that aspect of the *Miller* decision which would suggest that in order for constitutional protection to be extended, the information seized must be of a "personal and confidential" nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.

See also *Spencer*, paras 27-32.

2. What does law enforcement usually get as part of subscriber identity information? Do they also get national ID numbers?

In the financial context, subscriber data that can be obtained under the dedicated financial subscriber data production power described above (*Criminal Code*, section 487.018) includes: account numbers associated with a named person, names associated with a specified account number, details regarding the type of account, the status of the account, and the date on which the account was open or closed. Additional identification data can be obtained for identification purposes, which includes date of birth and current or historical addresses.

Canada does not have a national ID number. The closest corollary is the Social Insurance Number. However, under data protection principles of data minimization (encoded in Principle 4.3 of PIPEDA, which limits collection of personal data), telecommunications are generally precluded from collecting social insurance numbers as a condition of service, if other less-invasive means of identification are available (PIPEDA Case Summary #2001-22 [7]; PIPEDA Case Summary #2003-184 [8]; PIPEDA Case Summary #2003-204 [9]). As a result, telecommunications companies are unlikely to have Social Insurance Numbers on record for many customers.

Outside the definition in section 487.018 of the *Criminal Code* (which is limited to the financial context) there is no legal definition of subscriber information in Canada. Proposals have been advanced to define

the term, but not have yet to be adopted, most recently in a consultation document issued by the federal government in 2016, but also in past legislation:

> The consultation documents define basic subscriber information as "identifying information that corresponds to a customer's telecommunications subscription." The proposal does not specify a definitive list of identifying information that will be included in the power it proposes. However, past attempts to introduce warrantless access to subscriber information adopted the following legislative definition:
>
> > ... any information in the service provider's possession or control respecting the name, address, telephone number and electronic mail address [email address] of any subscriber to any of the service provider's telecommunications services and the Internet protocol address [IP address], mobile identification number, electronic serial number, local service provider identifier, international mobile equipment identity number [IMEI], international mobile subscriber identity number [IMSI] and subscriber identity module [SIM] card number that are associated with the subscriber's service and equipment. (Bill C-52, section 16)
>
> The consultation documents indicate that each of these identifiers could be included within the new power it contemplates, while acknowledging that indiscriminate warrantless access may be more appropriate for some of these identifiers than it is for others. However, in reality, most of the identifiers envisioned by this new power can have serious privacy implications deserving of protection.
>
> (https://citizenlab.org/wp-content/uploads/2016/10/20161005-CNSCI-RevisitingAnonymityYetAgain.pdf)

As indicated in the excerpt, legislated definitions will typically adopt a closed list of set customer identifiers. These have not historically included Social Insurance Numbers.

3. Is there any ex post requirement AFTER accessing subscriber identity information (for instance, is law enforcement required to notify the subscriber on whom they obtained the identity information of? Or is law enforcement required to destroy the information they obtained)?

There is no individual notification obligation attached to either the explicit financial subscriber information power encoded in the (*Criminal Code*, section 487.018), the general production power that is now the predominant vehicle for accessing subscriber data from communications providers (*Criminal Code*, section 487.014). Past legislative proposals for a dedicated 'subscriber data' power in the communications context have not included an individual notification obligation. However, the Supreme Court of Canada has recognized that the absence of safeguards such as an individual notification obligation can render a state surveillance practice unreasonable and hence in violation of section 8 of the *Charter*, particularly where such subscriber information is obtained without prior judicial authorization (such as in an emergency). See: *R v Tse*, [10]. See discussion in [11], Section Four A-ii, Individual Notice Obligation).

Canadian law has not yet recognized retention limitations as a constitutional obligation. Retention limitations could be implied under certain conditions from core constitutional principles (see discussion in [12], Section Three: c-iii, "Charter Principles of Incrementalism, Minimal Intrusion & Narrow Tailoring"). Canada's federal *public sector* data protection statute, the *Privacy Act*, RSC 1985, c P-21, does not currently impose an explicit retention limitation obligation onto state agencies. However, in a recently concluded statutory review of the *Privacy Act*, the House of Commons Standing Committee on Access to Information, Privacy and Ethics concluded that the Act should "be amended so as to explicitly require compliance with the criteria of necessity and proportionality in the context of any retention of personal information." ([13]. See also Recommendations 1 and 13).

4. Are subscribers allowed to find out from the communication service providers as to whether their information has been collected?

PIPEDA, Canada's federal private sector data protection regime, which applies to most communications access providers, recognizes an explicit right of individual access to personal information which extends to an organization's handling of that information:

> The access right is broad in scope. It is not limited in applicability to personal information collected from the individual, nor is its use limited to scenarios where an individual is exploring an organization's privacy practices.[222] It encompasses not only the existence of personal information, but extends to "an account of the use" of that information as well as of its disclosure to third parties.[223] This can include hand written notes regarding the requestor's account, phone call transcripts, board of director meeting records discussing the requestor, internal emails discussing the requestor, any video tapes of the requestor, and any opinions or performance evaluations issued relating to the requestor and based on their personal information.[224] Further, PIPEDA requires that the information be provided "in a form that is generally understandable."[225] This means that companies need not only provide a list of information to requesters, but must also explain that information and its context. An organization must, for example, explain the meaning of any customized markup the company has applied to the information for its uses. If requested, an organization must also generate transcripts for recorded phone calls between customer service representatives.[226]
>
> [222] PIPEDA Case Summary #2002-31; *Wyndowe v Rousseau*, 2008 FCA 39 (Federal Court of Appeal), para 9 ("He is entitled to…pursue his application, regardless of motivation.").
>
> [223] PIPEDA, Principle 4.9.1.
>
> [224] PIPEDA Case Summary #2011-003, http://www.priv.gc.ca/cf-dc/2011/2011_003_0325_e.asp (video tape); PIPEDA Report of Findings #2013-004, http://www.priv.gc.ca/cf-dc/2013/2013_004_0718_e.asp (internal emails); PIPEDA Case Summary #2004-285 (board of directors meeting); *Wyndowe v Rousseau*, 2008 FCA 39 (Federal Court of Appeal)(medical opinions by insurance company); PIPEDA Case Summary #2005-315 (time and date account password was changed as well as IP address used to do so).
>
> [225] PIPEDA, Principle 4.9.4.
>
> [226] PIPEDA Report of Findings #2012-010; PIPEDA Case Summary #2010-003, http://www.priv.gc.ca/cf-dc/2010/2010_003_0928_e.asp (change file format)
>
> SOURCE: Marina Pavlovic and Tamir Israel, "Canadian Consumers' Rights with Respect to Retail Telecommunications Services", Report for the Canadian Radio-television and Telecommunications Commission, April 27, 2014, pp 56-57

This includes information regarding disclosures of personal information made by a communications service provider to a state agency. (PIPEDA, sub-section 9(2.1))

Where the individual access demand implicates information relating to an organization's disclosure of personal information to facilitate a state investigation, the recipient state agency must first be notified and given an opportunity to veto the disclosure. (PIPEDA, sub-section 9(2.2)) Such a veto is only available to the organization where the organization is of the view that replying to the request could reasonably be expected to injure:

> (a) national security, the defence of Canada or the conduct of international affairs;

> (a.1) the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or
>
> (b) the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.
>
> PIPEDA, sub-section 9(2.3)

Telecommunications companies receiving such a request from a subscriber whose data has *not* been disclosed to law enforcement must notify the customer that no such disclosure has occurred. (PIPEDA Report of Findings #2016-008, [14). If disclosure to law enforcement *has* been made and the implicated state agency does not object, the individual is notified that disclosure has occurred. Where disclosure to law enforcement has occurred and the recipient state agency *vetos* notification, the individual is informed that "Our records reveal that either no such inquiry was made for [the telco's] account number: [XXXXXX] or that an inquiry was made and [the telco] is not permitted by the LEA to advise of this disclosure." (RoF 2016-008, para 11 [15]) The purpose of such a response is to avoid implicit confirmation to an individual that disclosure has occurred in spite of a determination by a state agency that the interests protected by PIPEDA sub-section 9(2.3) are engaged. However, that risk remains to the extent that an individual receiving such a reply is aware that the organization is obligated to affirmatively confirm all instances of non-disclosure. (See *Ruby v Canada (Solicitor General)*, [16], para 41). However, that risk is to some degree inherent in the legislative scheme as adopted. (RoF 2016-008, para 33)

The constitutionality of the current scheme is also in question. This is because a state agency's unilateral decision to invoke one of the exceptions encoded in PIPEDA sub-section 9(2.3) is highly insulated from any form of objective review. This is can be problematic to the extent that the individual access right encoded in PIPEDA is constitutional in nature. Canadian courts have recognized that section 2(b) of the *Charter*, which protects the freedom of expression, protects both 'speakers' and 'listeners' and encompasses a derivative right to receive information the absence of which 'would substantially impede meaningful public discussion and criticism on matters of public interest' or where the information sought is important for the exercise of an individual's *Charter* rights.

If applied in a manner that effectively shields important public debates from occurring regarding the appropriate scope of police practices, sub-section 9(2.3) may violate the Canadian *Charter*. (*R v Mentuck*, [17] para 51 "The improper use of bans regarding police conduct, so as to insulate that conduct from public scrutiny, seriously deprives the Canadian public of its ability to know of and be able to respond to police practices that, left unchecked, could erode the fabric of Canadian society and democracy."; *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, [18] para 37: "there is a *prima facie* case that s. 2 (*b*) may require disclosure of documents in government hands where it is shown that, without the desired access, meaningful public discussion and criticism on matters of public interest would be substantially impeded").

This would particularly be the case where the exception was invoked in an overbroad manner. The right to information is also strongly invoked where the information sought is important or necessary to the exercise of other constitutional rights. (*Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, [19] paras 28, 30 and 37: "PIPA prohibits the collection, use, or disclosure of personal information for many legitimate, expressive purposes related to labour relations. These purposes include ensuring the safety of union members, attempting to persuade the public not to do business with an employer and bringing debate on the labour conditions with an employer into the public realm. These objectives are at the core of protected expressive activity under s 2(b). … Expressive activity in the labour context is directly related to the Charter protected right of workers to associate to further common workplace goals under s 2(d) of the Charter."; *R v Tse*, [20] paras 82-86 ("Accountability for police use of

wiretapping without judicial authorization is important for s 8 purposes. In *Hunter v Southam*, Dickson J explained that "[a] provision authorizing . . . an unreviewable power would clearly be inconsistent with s 8 of the *Charter*""). Moreover, where constitutionally protected rights to liberty or security of the person are engaged under section 7 of the Canadian *Charter*, interference with these rights cannot be arbitrary or without due process (*Ruby v Canada (Solicitor General)*, [21] paras 167-173 "In a case such as this where an individual may not be fully aware of the information collected and retained by the government, the ability to control the dissemination of personal information is dependent on a corollary right of access, if only to verify the information's accuracy. In short, a reasonable expectation of access is a corollary to a reasonable expectation of privacy." (narrowed on appeal: *Ruby v Canada (Solicitor General)*, [22] paras 52-53); *John Doe Inc v Mukasey*, (US 2nd Circ)[23]). At minimum then, the lack of any judicial control over invocations of sub-section 9(2.3) may render the regime itself unconstitutional as it lacks any meaningful avenue for either the Privacy Commissioner or the Federal Court to review the validity of exemptions advanced by the state. (*Ruby v Canada (Solicitor General)*, [24], paras 41, 46-47)

5. Are there statistics on how many times such information access takes place?

The primary source of statistics with respect to subscriber information is the communications provider companies themselves, some of whom have undertaken to issue annual transparency reports that track requests. Two of Canada's three primary telecommunications companies (TELUS [25] and Rogers [26]) have done so since 2014. While not imposing any requirements to carry out such transparency reporting, the federal government has issued guidance on how organizations might do so if they choose: [27]). Canada's third and largest telecommunications company, Bell Canada, has not. In addition, the ongoing lack of consistency and robust definitions across companies limits the utility of these transparency initiatives. [28]

In addition, some snapshots of the scope of data access have been obtained by various means. For example, in response to a request from the Office of the Privacy Commissioner, the Canadian Wireless Telecommunications Association (CWTA) disclosed statistics aggregated from a large number of wireless and Internet access providers indicating 1.2 million data access requests were made in 2011, affecting an estimated 750,000 subscribers or accounts [29]. Some additional statistics regarding the practices of local policing services have been obtained by means of right to information requests (see [30]).

In addition, a recent legislative review of Canada's federal public sector data protection regime, the *Privacy Act*, recommended the adoption of a statistical reporting obligation to be imposed on the government covering lawful access requests made by law enforcement agencies: ([31] Recommendations 24 and 25)

[1] https://citizenlab.org/wp-content/uploads/2016/10/20161005-CNSCI-RevisitingAnonymityYetAgain.pdf
[2] SC 2000, c 5, http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html
[3] 2012 ONCA 660, https://www.canlii.org/en/on/onca/doc/2012/2012onca660/2012onca660.html
[4] 2014 SCC 43, [2014] 2 SCR 212, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do
[5] https://sustainability.telus.com/en/business-operations/transparency-report/
[6]http://about.rogers.com/2016/06/27/2015-rogers-transparency-report/ | http://www.rogers.com/consumer/privacy-crtc | http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf
[7] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/pipeda-2001-022/
[8] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-184/
[9] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-204/
[10] 2012 SCC 16, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/8002/index.do
[11] https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf
[12] https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf
[13] http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=e&Mode=1&Parl=42&Ses=1&DocId=8587799&File=78#a20
[14] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-008/
[15] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-008/
[16] 2002 SCC 75, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2017/index.do
[17] 2001 SCC 76, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1917/index.do
[18] 2010 SCC 23, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7864/index.do
[19] 2013 SCC 62, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13334/index.do
[20] 2012 SCC 16, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/8002/index.do
[21] [2000] 3 FCR 589 (CA), https://www.canlii.org/en/ca/fca/doc/2000/2000canlii17145/2000canlii17145.html
[22] 2002 SCC 75, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2017/index.do
[23] 549 F.3d 861, https://casetext.com/case/john-doe-inc-v-mukasey
[24] 2002 SCC 75, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2017/index.do
[25] https://sustainability.telus.com/en/business-operations/transparency-report/
[26]http://about.rogers.com/2016/06/27/2015-rogers-transparency-report/ | http://www.rogers.com/consumer/privacy-crtc | http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf
[27] https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/transparency-reporting-guidelines-2015.pdf/$file/transparency-reporting-guidelines-2015.pdf
[28] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032
[29] https://www.priv.gc.ca/media/1101/let_140430_e.pdf
[30] https://citizenlab.org/wp-content/uploads/2016/10/20161005-CNSCI-RevisitingAnonymityYetAgain.pdf
[31] http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=e&Mode=1&Parl=42&Ses=1&DocId=8587799&File=216#a66