R. *v.* Bykovets, 2024 SCC 6

"As a crucial component inherent in the structure of the Internet, an IP address is the key that can lead the state through the maze of a user's Internet activity and is the link through which intermediaries can volunteer that user's information to the state. Thus, [Section] *8 ought to protect IP addresses."* [**para. 13**]

Presentation by Asger and Jacob Vitus
Specialized Topics in Law 17 - Internet Law

Facts of the case - introduction

Background

- Calgary Police was investigating **fraudulent online purchase** that was happening from a liquor store back in 2017.
- The police found out, that the website used **Moneris** →Asked Moneris for the **IP address** of the fraudulent purchases, which was provided **voluntarily**.
- The police then used this information to obtain a **"*Spencer warrant*"** compelling the **IP addresses ISP**, Telus, to disclose **subscriber information, such as address and name**.
- Mr.Bykovest and his father was identified →Lead to **search warrant** and later arrest of Mr.Bykovest.
- Mr. Bykovest challenged the police request to obtain his IP address from Moneris, alleging that it **violated** his rights **against unreasonable search and seizure** under **section 8** of the Canadian Charter of Rights and Freedom.

Legal Framework

What was the case essentially about?

- The case revoked around whether or not the police, when asking Moneris about the IP address, should have gotten a prior **judicial authorization**, on the grounds that obtainment of Bykov IP address could be considered a search under **Section 8 of the Charter**
- What is a **search**? →A search occurs where the state invades a reasonable expectation of privacy. [Para 31]
- What is a **reasonable expectation of privacy** →When the **public interest of being left alone** outweighs **government's interest in advancing it's goal**, such as safety and security [Para 31]

Section 8 of the Charter:

- Section 8 →*Everyone has the right to be secure against unreasonable search or seizure."*
- To establish breach of section 8, two requirements must be meet (only requirement 1 was a issue in this case):
  - 1.There was a **search** or a seizure
  - 2.That **search** or seizure was **unreasonable**

Spencer Warrant

What is a Spencer Warrant?

- A judicial authorization that is needed before law enforcement could obtain information from IP addresses ISP.

Difference between Spencer and Bykovest case:

- Spencer →Got access to subscriber information with the use of IP address (Name, address and contact information).
- Bykovest →Only got access to IP address.
    - The reason why the police didn't get a *Spencer Warrant*, since no subscriber information was gathered.

Lower courts' decisions

Appellant's argument for the Superior Trial Court:

- Claimed police request to Moneris violated Section 8 of the Charter [unreasonable search & seizure].
- **Main issue**: Reasonable expectation of privacy in his IP address.

Superior Trial Court (2020 ABQB 70)	**Court of Appeal (2022 ABCA 208)**
● Ruled no reasonable expectation of privacy in IP addresses. ● IP addresses do not provide a direct link to a user or reveal personal info without third-party data.	● Agreed with lower court's analysis. ● **Dissent**: Argued the trial judge should have **focused on the identity linked to the IP**, which she felt created a reasonable privacy expectation.
Supreme Court Majority	
● Disagreed with lower courts. ● Emphasized that Charter rights must be **interpreted broadly**, protecting privacy fully.	

Issue for the Supreme Court - and the answer

Supreme Court's key question: Does a reasonable expectation of privacy attach to an IP address? [**para. 28**]

Supreme Court majority's answer: **Yes**, a reasonable expectation of privacy applies to an IP address.

Reasons for the Ruling:

- An IP address is the key link between an internet user and their online activities, including their identity.
- The IP address can reveal significant information about a user, even without a warrant.
- Limiting Section 8 protection to cases involving an IP address linked to a Spencer warrant overlooks the importance of the IP address itself.

The broader legal context:

- A narrow interpretation contradicts the broad, purposive approach required for privacy rights under Section 8 of the Charter.

The Rationale of the Majority of the Supreme Court (i)

When is there a breach of Section 8 of the Charter?

Section 8 of the Charter guarantees the right to be secure against unreasonable search or seizure.

Appellant's burden in a Section 8 claim: Must prove two things: i) **There was a search or seizure**, and ii) **the search or seizure was unreasonable**. In this case, the dispute focused only on whether there was a search.

What constitutes "a search"?

- Occurs when the state intrudes on a **reasonable expectation of privacy**.
- Privacy is reasonable if the public's interest in privacy outweighs the government's interest in law enforcement.

Assessing "privacy expectations": Courts consider **four factors** (4) [see table] to assess reasonable expectations of privacy.
*NB. In this case, only **factors 1 and 4** were at issue, as the parties agreed on the others.*

"Informational privacy":

- Focuses on "**informational self-determination**" – the right to control personal information.
- Individuals decide what personal information is shared, with whom, and under what conditions.

Privacy expectations - the four (4) factors ("the totality of circumstances test")
1) the subject matter of the search; 2) the claimant's interest in the subject matter; 3) the claimant's subjective expectation of privacy; and **4) whether the subjective expectation of privacy was objectively reasonable**

The Rationale of the Majority of the Supreme Court (ii)

The subject matter of the search (factor 1)

Key question in privacy cases:

- Courts must first identify the **subject matter** of the alleged search.
- "What were the police really after?" Courts must take a **broad, holistic view** of the search.

Defining "the search":

- Courts must be cautious when dealing with **electronic data**; it's not just about devices <u>but</u> the **data they hold**.
- In this case, police were seeking more than just an IP address - they wanted the **personal information** and **online activity** linked to them.

Broader implications of IP addresses:

- An IP address can link a user to specific internet activity, giving the state a tool to track **behavior over time**.
- Reflects the "technological reality" where privacy concerns are tied to both **data** and the **inferences** that can be drawn from it.

<u>Conclusion</u>: The IP address served as a key to uncover **highly personal information** about the user.

Appellant's argument
Police aimed to connect internet activity to a **specific person**, making the IP address crucial for identifying the user.
Crown's argument
Police were only after the **IP addresses** for their investigation.

The Rationale of the Majority of the Supreme Court (iii)

Was the expectation of privacy reasonable (factor 4)?

Section 8 of the Charter is triggered when an individual's **subjective expectation of privacy** is deemed **objectively reasonable**.

Balancing test: Courts weigh the **right to privacy** against the **government's need to intrude**, often for **law enforcement purposes**.

Case-by-case evaluation: Determined by evaluating several factors:

- **Control over the subject** of the search.
- **Place** of the search.
- **Private nature** of the information or material.

Let's dive into the different evaluation factors…

The Rationale of the Majority of the Supreme Court (iii.1)

Control over the subject matter (factor 4.1)

Informational privacy (and control):

- An individual's **control over their data** is not decisive in determining their **reasonable expectation of privacy**.
- Even when sharing information for a limited purpose or with specific groups (e.g., ISPs), privacy expectations can still exist.

Anonymity & online privacy [**paras. 46-47**]:

- **Anonymity** is a crucial aspect of privacy in the **online environment**.
- Privacy remains intact even when information is shared with third parties, such as ISPs, in contrast to the U.S. approach.

Internet users & privacy:

- Sharing subscriber information with ISPs is **unavoidable** for accessing internet services.
- However, this **does not eliminate privacy rights**.
- Canadians are not required to avoid using digital services to safeguard their privacy, as this would be **unrealistic and** unreasonable.

The Rationale of the Majority of the Supreme Court (iii.2)

The place of the search (factor 4.2)

Place of search and privacy: The **location** of the search is not crucial in determining a **reasonable expectation of privacy** for digital content.

Territorial v. digital privacy: Traditional **territorial privacy** principles don't apply well to digital subject matter, which is fundamentally different [**para. 49**].

Digital spaces:

- The **architecture of the internet** creates a broad, permanent, and expanding record of activity, unlike physical spaces [**para. 50**].
- **Online information** can reveal much more than data confined by physical limits.

Physical intrusion <u>not</u> required: The absence of **physical intrusion** does not diminish the expectation of privacy in the digital world.

The Rationale of the Majority of the Supreme Court (iii.3)

The private nature of the subject matter (factor 4.3)

Section 8 of the Charter protects an individual's **"biographical core of personal information"**, including intimate details of lifestyle and personal choices.

- Privacy is assessed **normatively**, beyond police intent, **safeguarding** dignity, autonomy, and personal growth.

Digital privacy [**paras. 54-56**]:

- Searches of computers and online data pose **heightened privacy concerns** due to the vast amount of personal information they reveal.
- **IP addresses** require strong protection in the digital age.

Societal realities: Decisions must account for the **pervasive nature of the internet** and its broader public consequences [paras. 58-59].

Flaws in the Crown's Argument:

1. IP addresses can reveal **personal information** before linking them to a user's identity. E.g., financial transactions like those tied to Moneris. Can also expose health concerns, sexual preferences, and political views [**paras. 60-63**].
2. IP addresses can be **correlated** with other data, revealing more about the user than initially sought. Websites like Google track **extensive personal data** [**para. 64-66**].
3. IP addresses can **lead to user identity** through online activities such as logging into social media. Relying on police or private companies for privacy protection is insufficient [**paras. 68-69**].

Meaning that…

- The **Spencer warrant** is not sufficient to address privacy concerns, thus…
- **IP addresses** must be treated as private due to their capacity to expose **highly personal information** in the modern digital world.

The Rationale of the Majority of the Supreme Court (iii.4)

Does the balance weigh in favour of a reasonable expectation of privacy? (factor 4.4)

A balance between individual privacy and society needs for safety and security [para 71]

- Individual privacy: Used the same arguments as in factor 4.3 →The IP address with the help of third-party companies such as Google, **can** lead the state directly to a user's identity through their online activities. [Para 74-80]
- Safety and security: With the ever evolving technology, the police should have the adequate tools to solve the crime the evolving technology brings. [Para 84]

Ruling →There was a reasonable expectation of privacy in regards to the IP address (5 to 4 decision)

Grounds:

- The requiring of judicial authorization before acquiring an IP address is first of all not **an onerous investigative step**, and it would not unduly interfere with **law enforcement's ability to deal with this crime**. [Para 85]
- A reasonable expectation of privacy also significantly reduces the potential of **any "arbitrary and even discriminatory**" exercises of discretion that would empower the state to identify information about any Internet user it pleases for any reason it sees fit [Para 87]
- Lastly by adding **judicial oversight** it removes the decision of what and how much information that should be disclosed **from the private companies and returns it to the purview of the charter**.[Para 89]

"Extending s. 8's reach to IP addresses protects the first "digital breadcrumb" and therefore obscures the trail of an Internet user's journey through the cyberspace." [Para 91]

Dissent in the Supreme Court's decision (i)

The subject matter of the search (factor 1)

- *Dissent disagreed with the majority approach →Concluded that the subject matter of the search* was the IP addresses, I.e, the collections of numbers, and the identity of the ISP that is revealed by them. [Para 140]

- Argument from the Dissent→The ultimate goal of the investigation was to reveal the suspect, but the IP address from Moneris didn’t in iftself do that. [Para 128]

Dissent in the Supreme Court's decision (ii)

Factor 4.1 →Control Over the Subject Matter

- Dissent →The appellant in the case did have little control over his IP address. An Internet user who leaves behind IP address data completely loses control over what happens to those numbers.[153-154]
- No control of IP address →Points away from the finding that expectation of privacy was reasonable. [Para 155]

Factor 4.2 →Place of the Search

- Dissent → The digital location of the search does not enhance the objective reasonableness of the appellant subjective expectation of privacy.

Factor 4.3 →Private Nature of the Subject Matter

- Dissent → The case should be based on evidentiary record and nothing else[Para 149].
- The IP address in the case wasn't private and didn't reveal any personal information →Points away from the finding that any expectation of privacy was reasonable. [Para 151]

Factor 4.4 →Conclusion on Reasonable Expectation of Privacy

- Dissent →Based on the facts above, the dissent found, that the appellant didn't have any reasonable expectation of privacy. [Para 158]
- Warned against that the ruling would counter worked the police ability to investigate serious crimes, especially against children [Para 159-160]

"With the utmost respect, I believe that the effect of my colleague's reasoning is to answer a question that is not asked, on the basis of factual scenarios different from the one in this case, in order to address a social problem that is not in issue here. I would say nothing more on this, so as not to prejudge the matter should it ever arise." [Para 164]

Key takeaways

- IP address in itself creates a reasonable expectation of privacy.

- Double downed on *Spencer* →The SCC extended the obligation of getting a judicial authorization to now apply when the state is requesting IP addresses.

- The constitutional right to privacy would no longer be based on the state's declared intention in regards to the information sought→Now based on what the information gained tends to reveal, when the information is pieced together with other information.

- The SCC recognizes the expanding role of third-party digital companies in regards to the relationship between state and individual, which is made possible due to the internet.