METADATA RETENTION AND THE LIMITS OF STATE POWER

*Tee May Ern**

Introduction

The retention of data by states has gained growing importance in recent decades, often as a means of combating crime, but capable also as a tool for exerting control over the country. Advances in technology have transformed the ability to collect vast amounts of data from a costly and complex undertaking into a relatively inexpensive and effortless process. This article focuses on one particular category of data — metadata — which captures information about communications rather than their content. Examples include the time, date, and duration of a phone call, the recipient's number, or the location from which an email was sent. Importantly, it does not include the content of such communications.

This article examines two landmark decisions of the Court of Justice of the European Union (CJEU), Digital Rights Ireland[1] and Tele2 Sverige[2], which together have defined the limits on state power to retain metadata. These cases are chosen not only because the CJEU is at the forefront of developing clear, rights-focused principles on data protection, but also because its rulings are grounded in the General Data Protection Regulation (GDPR), which is widely regarded as the global gold standard in data protection law. Though decided based on an EU legal framework, the reasoning in these cases offer valuable insights for other jurisdictions, where similar tensions between individual rights and state authority are increasingly relevant.

From Targeted Surveillance to Metadata Retention

There is little doubt that most surveillance methods interfere, to varying degrees, with the right to privacy and private life. Across jurisdictions, measures such as video surveillance and the interception of private communications have been almost uniformly recognised as infringing these rights.[3] Such traditional forms of surveillance share a common feature: they are targeted,

* Lecturer, Faculty of Law and Government, HELP University

[1] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ECLI:EU:C:2014:238.

[2] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige, Watson and Others* EU:C:2016:970.

[3] See, for example: *Allan v United Kingdom* (2003) 36 E.H.R.R. 12; *Köpke v German* [2010] 10 WLUK 58; *Antović and Mirković v Montenegro* [2017] 11 WLUK 675; *Klass and others v Germany* (1978) 2 EHRR 214; *Liberty and others v United Kingdom* (2009) 48 E.H.R.R. 1; *Kennedy v UK* [2010] 5 WLUK 411; *Roman Zakharov v Russia* (2016) 63 E.H.R.R. 17.

and typically directed at individuals who are suspected of, or charged with, committing crimes. In this sense, they align neatly with the conventional purpose of surveillance, which is commonly the justification relied on by states for carrying out data retention measures, since it focuses on retaining data of those who are considered to be suspects, rather than that of everyone.[4]

At issue in this article, however, is a form of surveillance that diverges sharply from said traditional forms of surveillance. Metadata retention by states typically involves retaining information on everyone's communications, irrespective of whether they are, or have ever been, suspected of a crime. This makes metadata retention distinct from traditional surveillance in two significant respects. First, it is often argued to be less intrusive because it concerns only the fact of communication, not its substance.[5] Secondly, metadata retention is often collected indiscriminately, covering the entire population of a country, rather than being confined to suspected individuals, a feature that departs fundamentally from the conventional idea that surveillance must be targeted. These differences underscore that, unlike traditional methods, metadata retention poses its own distinct challenges for the protection of fundamental rights.

The Digital Rights Ireland decision

The case of Digital Rights Ireland concerned the lawfulness of the Data Retention Directive[6], which required all telecommunications service providers to retain metadata for a period between six and twenty-four months. This general and indiscriminate retention provision, applied for the stated purpose of the "investigation, detection and prosecution of serious crime,"[7] was challenged to be incompatible with Articles 7, 8 and 11 of the Charter of

[4] 'Surveillance, n.: Watch or guard kept over a person, etc., esp. over a suspected person, a prisoner, or the like' *Oxford English Dictionary* (OUP 2025) (OED Online) <https://www.oed.com> accessed 18 August 2025.

[5] Governments have frequently downplayed the intrusiveness of metadata retention with remarks such as "*it's just metadata*," "*nobody is listening to your phone calls*," or "*nobody is reading all your emails*," stressing that the content of communications is not retained and that metadata is therefore not revealing. See, for example, statement by former US Chair of the Senate Intelligence Committee, Dianne Feinstein, in Naughton, 'NSA surveillance: don't underestimate the extraordinary power of metadata' *The Guardian* (June 2013) <https://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama> accessed 18 August 2025; statement by former US President, Barack Obama, '"Nobody is listening to your telephone calls," Obama says,' *CBS News* (June 2013) <https://www.youtube.com/watch?v=hUD1ujK2BJc> accessed 18 August 2025; statement by former GCHQ Director, Sir David Omand, 'Ex-GCHQ chief: 'Nobody is reading all your emails'' *BBC News* (October 2013) <https://www.bbc.co.uk/news/av/uk-24454918/ex-gchq-chief-nobody-is-reading-all-your-emails> accessed 18 August 2025.

[6] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (now invalidated by Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ECLI:EU:C:2014:238).

[7] Art 1(1) of the Data Retention Directive (now invalidated).

Fundamental Rights of the European Union, which respectively protect the rights to private life, protection of personal data, and freedom of expression.

At the very outset of its judgment, the Court made a striking observation that metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained"[8] and may "generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[9] The placement of this statement at the beginning of the judgment underscored the Court's recognition that the retention of metadata, even absent content, poses a serious and inherent risk to privacy. It set the tone for a strict and sceptical review of the Directive's compatibility with fundamental rights.

The Court had little difficulty concluding that the Data Retention Directive interfered with the rights to privacy and data protection in a "wide-ranging" and "particularly serious" manner,[10] which led to the central issue on whether such interference was proportionate. While the Court accepted that the Directive pursued a legitimate objective of general interest, namely, that of fighting crime, particularly organised crime, it held that the measure went beyond what was strictly necessary to achieve that aim.

First, the Directive applied in a generalised and indiscriminate manner to all persons and all means of electronic communication, regardless of whether individuals had any connection, even an indirect or remote one, to serious crime.[11]

Second, it failed to include substantive and procedural safeguards governing access to and use of the retained data: it did not define "serious crime",[12] did not restrict the number of authorised personnel to the minimum necessary,[13] and did not make access conditional on prior review by a court or an independent administrative body.[14]

Third, the Directive did not distinguish between categories of metadata according to their investigative value, nor did it require a determination of retention period based on any objective

[8] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ECLI:EU:C:2014:238 at [27].
[9] Ibid, [37].
[10] Ibid.
[11] Ibid, [57] and [59].
[12] Ibid, [60].
[13] Ibid, [62].
[14] Ibid, [62].

criteria.[15]

Lastly, the Directive did not ensure an adequately high level of data security, as it allowed providers to weigh economic considerations in determining safeguards,[16] failed to guarantee the irreversible destruction at the end of the retention period,[17] and did not require that the collected data be retained within the EU.[18]

Consequently, the Directive was found to be disproportionate and contrary to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, and as a result, declared invalid. In doing so, the Court made it very clear that any metadata retention regime must be accompanied by a rigorous and comprehensive system of checks and balances, including precise definitions of scope, strict necessity tests for different data categories, objectively justified retention periods, independent prior authorisation for access, and robust data security. The Court had applied the proportionality test stringently in this area, setting a demanding benchmark for future cases. It effectively demanded that Member States not only pursue legitimate objectives, but also adopt the least rights-intrusive means available, with safeguards designed to reduce any encroachment on privacy or data protection rights to the absolute minimum.

From Digital Rights Ireland to Tele2 Sverige

Following Digital Rights Ireland and its invalidation of the Data Retention Directive, it remained theoretically possible for Members States to maintain and enact national laws which mandate a general and indiscriminate data retention, provided that the strict safeguards laid down by the CJEU in Digital Rights Ireland were met. The Tele2 Sverige case was one which sought clarification on whether such national laws were compatible with Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union, as well as Article 15(1) of the ePrivacy Directive (2002/58/EC). Specifically, one of the central issues was whether all the safeguards identified in Digital Rights Ireland were compulsory, or whether Member States could cherry pick among them in designing their own data retention regimes.

In Tele2 Sverige, the Court made clear that every safeguard in Digital Rights Ireland was

[15] Ibid, [63]-[64].
[16] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others ECLI:EU:C:2014:238, at [67].
[17] Ibid.
[18] Ibid, [68].

mandatory, and that Member States cannot take any one safeguard more seriously in order to make up the fact that they have neglected another.[19] Crucially, the Court went further than it did in Digital Rights Ireland to hold that any regime of general and indiscriminate retention is inherently disproportionate.[20] Such measures, it reasoned, affect all individuals, regardless of any link, even indirect, to criminal proceedings,[21] and make no exceptions for persons bound by professional secrecy, such as lawyers or journalists.[22] The Court confirmed that retention could still be lawful, but only where it is genuinely targeted and strictly necessary. This requires limitation by reference to the categories of data retained, the means of communication affected, the persons concerned, and the retention period.[23] As an example, the Court suggested a model of targeted retention based on specific geographical areas with demonstrably high crime risk.[24]

Reflections on the CJEU's Data Retention Jurisprudence and Its Wider Implications

The decision of Tele2 Sverige clearly demonstrates a strong and uncompromising judicial stance in the matter of data protection through the setting of minimum, non-negotiable standards governing the retention of metadata. In doing so, the CJEU has re-calibrated the constitutional balance between security consideration and fundamental rights protection, tilting it decisively in favour of the latter. Nevertheless, the rulings also raise several practical and operational challenges which cannot be neglected.

One of the natural consequences of the Tele2 Sverige ruling, which prohibited all forms of general and indiscriminate data retention, is the curtailment of the investigative capacities of law enforcement authorities. In many cases, the police cannot know in advance which data will prove relevant or who the perpetrators of crimes will be. Being able to collect first and then access later gives law enforcement the benefit of going back in time to identify associates, track movements, tie suspects to crime scenes, expose other unidentified offenders, and test the consistency of accounts given by suspects or victims.[25]

[19] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige, Watson and Others* EU:C:2016:970, at [125].
[20] Joined Cases C-203/15 and C-698/15, Tele2 Sverige, Watson and Others EU:C:2016:970, at [103].
[21] Ibid, [105].
[22] Ibid.
[23] Ibid, at [108].
[24] Ibid, [111].
[25] Iain Cameron, 'Balancing data protection and law enforcement needs: Tele2 Sverige and Watson' (2017) Common Market Law Review 1467; Sir Anthony May, *Report of the Interception of Communications Commissioner* (HC 1113, 2005), para 7.65 <https://privacyinternational.org/sites/default/files/2018-02/4.%20GCHQ%207.pdf> accessed 18 August 2025.

The counterargument, of course, is that such general retention measures contribute little in practice. In many high-profile attacks, the perpetrators were already known to the authorities, who simply failed to monitor them effectively.[26] Moreover, the sheer volume of indiscriminately retained data may dilute its evidential value, making a well-targeted regime more effective in practice.

However, the targeted retention model endorsed in Tele2 Sverige is deeply flawed and risks creating new problems. The Court stated only an "indirect" link to serious crime is needed to trigger retention,[27] and suggested a targeted retention model based on geographical location.[28] Notably, the term "indirect" suggests a threshold lower than the usual standard of reasonable suspicion, thereby signalling a relatively minimal evidentiary requirement. This leaves the door open to sweeping, city-wide retention orders, such as retaining the data of all residents of London, which would still capture vast swathes of people with no connection to serious crime. In effect, we risk replacing one form of indiscriminate retention with another, only on a marginally smaller scale.

Worse still, targeted retention can magnify the intrusiveness of surveillance, unjustly subjecting innocent individuals to stigma and further eroding their presumption of innocence. Further, if the targeted area happens to be home to a disproportionately high number of people from a particular community, such as Muslims or immigrant populations, the practice risks evolving into geographical profiling and indirect forms of discrimination. Paradoxically, a general retention regime may, in some respects, be less discriminatory, since any resulting harm is spread across the whole population.

Ultimately, replacing general retention with targeted retention risks being a superficial fix that solves one problem on the surface while creating others that could be just as serious, if not more so. In this author's view, the Digital Rights Ireland decision struck the more sensible balance by allowing general retention under the condition that it met stringent safeguards and robust oversight mechanisms. This would have preserved investigative utility while minimising rights infringements to the greatest extent possible, and at the same time, afford

[26] Jamie Grierson, 'Police and MI5 missed chances to prevent Manchester bombing, MPs find' *The Guardian* (22 November 2018) <https://www.theguardian.com/uk-news/2018/nov/22/police-and-mi5-missed-chances-to-prevent-manchester-arena-bombing-mps-find> accessed 18 August 2025; 'London Bridge inquests: Chances 'galore' to stop attack, says lawyer' *BBC News* (31 May 2019) <https://www.bbc.co.uk/news/uk-48476417> accessed 18 August 2025.
[27] Joined Cases C-203/15 and C-698/15, Tele2 Sverige, Watson and Others EU:C:2016:970, at [111].
[28] Ibid.

Members States greater flexibility to tailor data retention measures in response to specific security threats.

Conclusion

This article argues that while the Tele2 Sverige ruling was driven by a legitimate concern for privacy, it overreaches and creates significant new risk. By prohibiting all forms of general data retention, it removes a valuable investigative tool in the fight against serious crime, replacing it with a targeted model that may unjustly single out innocent individuals, foster discriminatory outcomes, and, paradoxically, lead to more intrusive surveillance. These practical implications cannot be ignored; if left unaddressed, they risk rendering data retention frameworks an exercise in theoretical detachment, whereby standards are commendable in theory yet incapable of practical realisation. The pressing task is not, and should not be, to abolish general and indiscriminate retention altogether, but to establish a regime that both protects privacy and preserves the operational effectiveness of law enforcement. In this regard, the Digital Rights Ireland decision achieved a more proportionate balance, recognising that general retention can be compatible with fundamental rights when accompanied by strict safeguards and robust oversight, thereby offering a more workable approach.