DELIVERABLE 11.3

OEI – REQUIREMENT NO. 3

WORK PACKAGE NUMBER: 11

WORK PACKAGE TITLE: ETHICS REQUIREMENTS

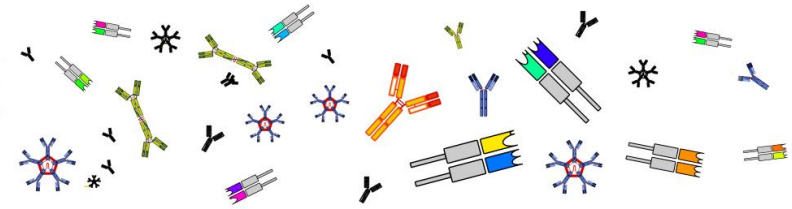
This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

Document Information

iReceptor Plus Project Information	
Project full title	Architecture and Tools for the Query of Antibody and T-cell Receptor Sequencing Data Repositories for Enabling Improved Personalized Medicine and Immunotherapy
Project acronym	iReceptor Plus
Grant agreement number	825821
Project coordinator	Prof. Gur Yaari
Project start date and duration	1st January, 2019, 48 months
Project website	http://www.ireceptor-plus.com

Deliverable Information	
Work package number	11
Work package title	Ethics requirements
Deliverable number	D11.3
Deliverable title	OEI – Requirement No. 3
Description	Data will be exchanged with the US. Band with neutrality having been repelled, there is a direct impact on data velocity which can influence data use and visibility, both aspects being paramount to big data approaches. This issue must be considered and mitigated by the participants.
Lead beneficiary	1-BIU
Lead Author(s)	Jos Dumortier
Contributor(s)	Liesa Boghaert

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



Revision number	3
Revision Date	31 March, 2019
Status (Final (F), Draft (D), Revised Draft (RV))	F
Dissemination level (Public (PU), Restricted to other program participants (PP), Restricted to a group specified by the consortium (RE), Confidential for consortium members only (CO))	CO

Document History

Revision	Date	Modification	Author
1	25/03/19	First draft	Jos
2	25/03/19	Review/edit	Brian
3	28/03/19	Review/edit	Bracha

Approvals

	Name	Organisation	Date	Signature (initials)
Coordinator	Prof. Gur Yaari	Bar Ilan University	31 Mar, 2019	GY
WP Leaders	Prof. Gur Yaari	Bar Ilan University	31 Mar, 2019	GY

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

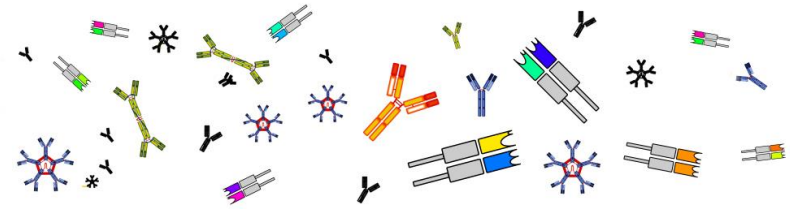
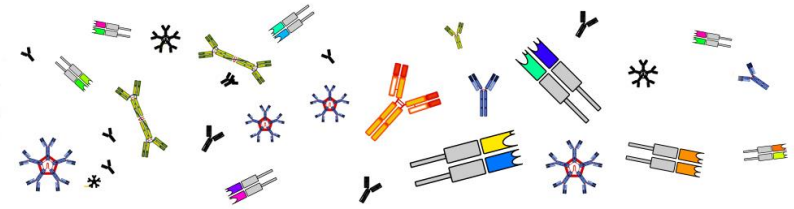


Table of Contents

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

iReceptor+

Executive Summary



This deliverable provides an assessment of the potential impact of the 2018 US Federal Communications Commission's 'Restoring Internet Freedom Order', which repealed the net neutrality rules previously installed under the Obama administration.

In doing so, this deliverable first defines the concept of net neutrality and provides an overview of the positions that the European Union, Canada, Israel and the United States of America take in the net neutrality debate.

The document then proceeds by examining the potential implications of the regulatory rollback on the iReceptor Plus platform, which is considered rather low, if any at all. This impact assessment was based on the findings that:

(1) The repeal of net neutrality in the US might be overturned soon, as a consequence of the bill introducing the '2019 Save the Internet Act' or of the petition for review signed by attorneys-general from 22 States (see further in this deliverable);

(2) If the repeal of net neutrality is not overturned at the federal level, state legislation might still enforce the net neutrality principle;

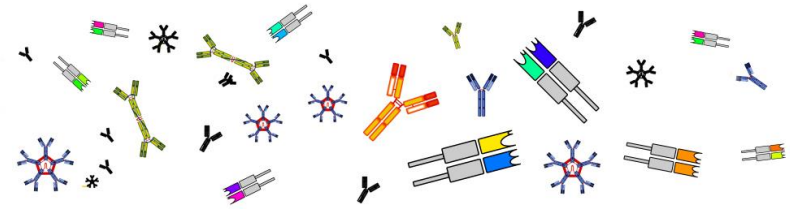
(3) The repeal of net neutrality in the US can only potentially affect a small number of partners and end-users in the iReceptor Plus project, given that only commercial ISPs (as opposed to 'academic networks') would eventually abandon net neutrality,

(4) The potential lowering of internet speed as a consequence of the repeal of net neutrality, will not gravely hinder the visibility or use of data, since big data analysis operations performed through the iReceptor platform are not very time-critical;

(5) Any potential risk of data vulnerability or lack of data privacy is diminished by the extraterritorial application of the obligations arising from the EU General Data Protection Regulation.

Furthermore, in terms of impact mitigation, the deliverable proposes to rely on educational or research networks to the greatest extent possible, both when hosting and accessing the AIRR-sequence data repositories. To this end, partners and end-user could make us of VPN-networks or could directly subscribe to academic networks (where possible). If such measures are not available, partners and end-users should rely only on commercial ISPs that provide sufficient guarantees with regard to data velocity, security and privacy.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



1. Introduction

1.1 Purpose of the deliverable

As a part of work package 11 (Ethics requirements), Deliverable 11.3 is dedicated to the recent, much debated rollback of bandwidth neutrality in the United States of America (US) under the Trump administration. The purpose of the deliverable is to consider, assess and mitigate the potential impact of this repeal of bandwidth neutrality on the access to and the use of the Adaptive Immune Receptor Repertoire sequence data (AIRR-seq data) repositories through the iReceptor Plus platform.

1.2 Concept of net neutrality

Prior to evaluating the potential impact of the regulatory rollback in the US on the iReceptor Plus project, it is worth briefly recalling the concept of net neutrality. Bandwidth or network neutrality, commonly referred to as 'net neutrality', is a term first coined by prof. TIM WU[1]. It refers to the principle that Internet Service Providers (ISPs)[2] and governments should treat all data on the internet the same, not prioritizing traffic, or charging differentially by priority status, or imposing congestion charges.[3]

In essence, the net neutrality debate revolves around the question if ISPs should be able to use network infrastructure to discriminate between data packets which travel across their networks for commercial or policy reasons as opposed to network performance reasons. Present-day technologies enable ISPs to favour data packages which originate from a preferred source and deprioritise or even block packets from non-preferred sources. This process, called 'access tiering', enables ISPs to create different levels of service quality to content providers and engage in differential pricing and price discrimination.

Proponents of net neutrality argue that government intervention is essential to guarantee the 'end-to-end' design of the internet and maintain that access tiering will jeopardise the future of innovation online. Opponents of net neutrality on the other hand, contend that the ever-

[1] T. WU, "Network Neutrality, Broadband Discrimination", *Journal of Telecommunications and High Technology Law* 2003, Vol. 2, 141.

[2] Although strictly speaking, the net neutrality debate relates to Internet Access Providers (IAPs), in this Deliverable the more commonly used generic term ISPs will be used, except for when legislative documents are cited.

[3] R. LEE and T. WU, "Subsidizing Creativity through Network Design: Zero-Princing and Net Neutrality", *Journal of Economic Perspectives* 2009, 23(3), 61-76.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

increasing demands placed on modern internet require a level of investment and innovation that can only be established if the internet is efficiently commercialised. This would, according to them, in the long run be to the benefit of all consumers.

2. Overview of regulatory frameworks on net neutrality

Although the final objective of the iReceptor Plus project is to develop an innovative platform that integrates distributed repositories of AIRR-seq data from around the world, the iReceptor Plus project currently includes twenty consortium partners, originating from the European Union, Canada, Israel and the US. Therefore, it is useful to not only delve into the state of the net neutrality debate in the US, but to also look at the position that the European Union, Canada and Israel adopt in this regard.

2.1 The European Union

In the European Union, the principle of net neutrality is enshrined in the 'Regulation (EU) 2015/2120 laying down measures concerning open internet access'[4]. This 'EU Open Internet Regulation' aims at establishing common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-user's rights. It seeks to protect end-users and simultaneously guarantee the continued functioning of the internet ecosystem as an engine of innovation.[5]

In pursuing these aims, the Open Internet Regulation grants end-users a right to access and distribute the lawful content and services of their choice via their internet access service.[6] Moreover the Regulation obliges ISPs to treat all internet traffic equally, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.[7] Reasonable traffic management however remains allowed if necessary safeguards are complied with. Specialised services that assure a specific quality level required for certain content, applications or services (such as connected cars or 5G applications) can still be offered as well.

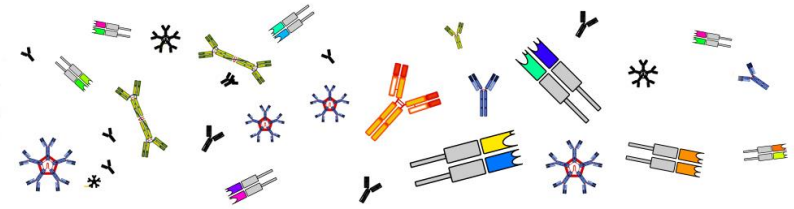
[4] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union

[5] Recital 1 of the Open Internet Regulation, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2120

[6] Article 3(1) of the Open Internet Regulation.

[7] Article 3(3) of the Open Internet Regulation.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



In any case, ISP must comply with several transparency obligations that inform end-users on traffic management measures and their impact on the use of content, applications and services.[8]

In order to guarantee adequate supervision and enforcement, the Open Internet Regulation instructs national regulatory authorities (NRA's) to monitor and ensure compliance with the provisions cited above. To this end, the Body of European Regulators for Electronic Communications (BEREC) issued guidelines for NRA's on the implementation of the European net neutrality rules.[9]

2.2 Canada

In Canada the debate on net neutrality has been settled in favour of an open internet as well. In this context, the Canadian Telecommunications Act stipulates[10]:

27(2) "*No Canadian carrier shall, in relation to the provision of a telecommunications service or the charging of a rate for it, unjustly discriminate or give an undue or unreasonable preference toward any person, including itself, or subject any person to an undue or unreasonable disadvantage*."

36 "*Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public*."

The 'Commission' mentioned in the above provision, refers to the Canadian Radio-television and Telecommunications Commission (CRTC), which examines ISP practices on a case-by-case basis, in response to a complaint or on its own initiative. In this context, the CRTC enacted two policies[11] for determining whether a fixed or mobile ISP acts consistently with sections 27(2) and 36 of the Act, specifically regarding internet traffic management practices and differential pricing practices.

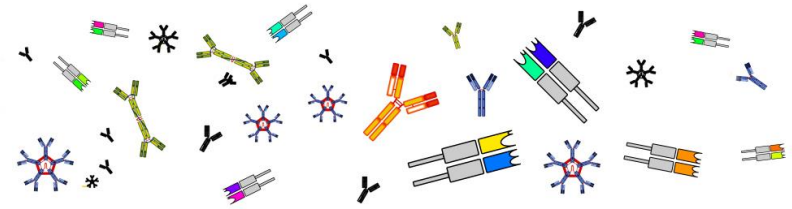
[8] Article 4 of the Open Internet Regulation.

[9] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, available at: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

[10] Canadian Telecommunications Act – S.C. 1993, c. 38 (Section 27 and 36), available at: https://laws-lois.justice.gc.ca/eng/acts/T-3.4/

[11] Telecom Regulatory Policy CRTC 2009-657 (available at: https://crtc.gc.ca/eng/archive/2009/2009-657.htm) and Telecom Regulatory Policy CRTC 2017-104 (available at: https://crtc.gc.ca/eng/archive/2017/2017-104.htm).

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



It is furthermore expected that the principle of net neutrality will be continuously and increasingly safeguarded in Canadian law in the future, given that the Canadian Parliament on 23 May 2018 unanimously called on the Government to "explore opportunities to further enshrine in legislation the principles of neutrality in the provision and carriage of all telecommunications services"[12]. Acting on this request, the Canadian Government on 28 June 2018 requested the expert panel conducting the Broadcasting and Telecommunications Legislative Review to examine if current legislative provisions are well-positioned to protect net neutrality principles in the future.[13] The Panel's final report and recommendations are due 31 January 2020.[14]

2.3 Israel

In Israel, net neutrality for mobile broadband providers has been incorporated in the law in 2011. This principle was expanded to wireline broadband providers in 2014. Besides that, clause 29 of Israeli Communications Law (Telecommunications and Broadcasting) considers "obstructing, preventing or hindering the sending or the delivering of a Telecommunication Message in any way whatsoever" a criminal office.[15]

2.4 The United States of America

In the US, net neutrality has been a contentious issue for years. The focus of the net neutrality debate in the US relates to the question if the broadband internet access market should be regulated under strict net neutrality rules that impose a ban upon the contested practices of blocking[16], throttling[17] and paid prioritization[18] or if a light-touch regulatory approach would be more appropriate.

[12] https://www.ourcommons.ca/DocumentViewer/en/42-1/house/sitting-299/journals

[13] https://www.ic.gc.ca/eic/site/110.nsf/vwapj/terms_of_reference_EN.pdf/$FILE/terms_of_reference_EN.pdf

[14] https://www.canada.ca/en/canadian-heritage/news/2018/06/government-of-canada-launches-review-of-telecommunications-and-broadcasting-acts.html

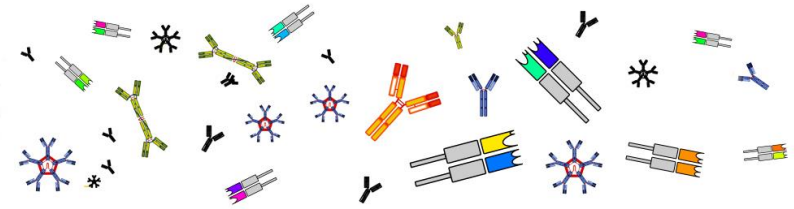
[15] See translation by the World Intellectual Property Organization (WIPO), available at: https://wipolex.wipo.int/en/text/348019

[16] Blocking refers to the practice in which consumers who subscribe to a retail broadband Internet access service do not get access to all (lawful) destinations on the Internet.

[17] Throttling refers to the practice in which lawful content, applications, services, and devices are degraded or impaired by ISPs.

[18] Paid prioritization refers to the practice in which ISPs accept payment (monetary or otherwise) to manage their network in a way that benefits particular content, applications, services or devices.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



Under the Obama administration, a first attempt to regulate net neutrality in the US was made with the 2010 'Open Internet Order'[19]. This order was however overturned by court in 2014, following a lawsuit by US network operator Verizon, who claimed that the American telecommunications regulator, the Federal Communications Commission (FCC) had no authority to enforce network neutrality rules, as long as ISP's were not identified as 'common carriers.' Therefore, in a new 2015 'Open Internet Order'[20], the FCC reclassified broadband internet access services as 'telecommunications services' under Title II of the Communications Act. The Open Internet Order also adopted bright-line rules that prohibited blocking, throttling and paid prioritization, as well as a General Conduct Rule and a Transparency Rule.

In 2018 however, under the Trump administration, the FCC issued the 'Restoring Internet Freedom Order'[21] which repealed the previously installed net neutrality rules to promote broadband investment. It does however retain a transparency rule, which requires ISP's to publicly disclose information regarding their network management practices, performance, and commercial terms of service.

The 'Restoring Internet Freedom Order' is however heavily criticized. Attorneys general from 22 states filed a protective petition for review against the FCC in the U.S. Court of District Columbia[22] and thirty-four states as well as the District of Columbia introduced 120 bills and resolutions regarding net neutrality in the 2018 legislative session. Five states (California, New Jersey, Oregon, Vermont and Washington) moreover enacted legislation or adopted resolutions maintaining net neutrality rules.[23]

Furthermore, the Democrats in the House and Senate have introduced 'the Save the Internet Act of 2019' bill[24] which aims at restoring the FCC's Open Internet Order of 2015 and its net neutrality protections. As such, the bill proposes to repeal the 'Restoring Internet Freedom

[19] US FCC, Report and Order, In the Matter of Preserving the Open Internet; Broadband Industry Practices; GN Docket No. 09-191, WC Docket No. 07-52, 23 December 2010, available at : https://docs.fcc.gov/public/attachments/FCC-10-201A1_Rcd.pdf

[20] US FCC, Report and Order, In the matter of Protecting and Promoting the Open Internet; GN Docket No. 14-28, 12 March 2015, http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf

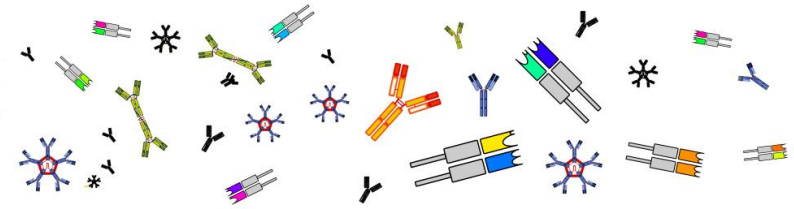
[21] US FCC, Report and Order, In the Matter of Restoring Internet Freedom, WC Docket No. 17-108, 4 January 2018, available at: https://docs.fcc.gov/public/attachments/FCC-17-166A1.pdf

[22] Available at: https://ag.ny.gov/sites/default/files/petition_-_filed.pdf

[23] http://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-legislation-in-states.aspx

[24] Available at: https://www.markey.senate.gov/imo/media/doc/Save%20The%20Internet%20Act%20of%202019.pdf

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



Order' of 2018 and prohibits the issuing of an Order with similar content in the future. The bill will be voted in April 2019.

2.5 Conclusion

In conclusion, the principle of net neutrality is strongly supported in the EU, Canada and Israel. Moreover, this support has been recently intensified through the enhanced cooperation between the EU and Canadian regulators (respectively BEREC and CRTC) in the context of net neutrality, as part of a Memorandum of Understanding in October 2018.[25] In the US the net neutrality dispute was recently decided in disadvantage of net neutrality. Nevertheless, due to heavy criticism in many states and by the Democrats in the House and Senate, it is far from certain whether the repeal of net neutrality rules will hold in the future.

C. Impact of the regulatory rollback in the US for iReceptor Plus

§1. Potentially affected end-users

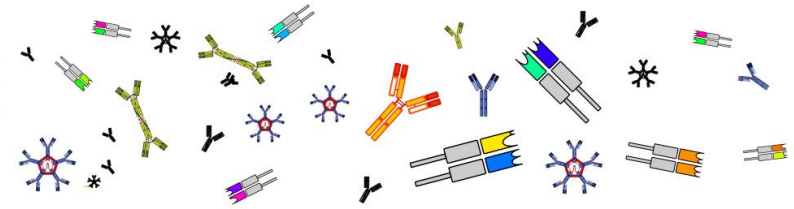
When examining the impact of the recent repeal of net neutrality rules in the US on iReceptor Plus, it is crucial to first assess which end-users of the platform could be affected. In that context, it should be emphasised that the 2018 'Restoring Internet Freedom Order', which rolls back previous net neutrality rules, from a technical point of view, can only affect the access to and the use of the iReceptor Plus platform if an American commercial ISP is involved in the carrying of the data packets. If data are communicated through educational or research networks ('academic networks'), however, these communications will not be affected, given that these networks are separate, non-commercial networks, that do not engage in access tiering.

Applied to the iReceptor Plus project, this means that only in two instances the repeal of net neutrality rules in the US might affect the access to and use of the platform. This is firstly when end-users anywhere in the world are accessing data repositories that are run by a non-academic partner relying on an American commercial ISP that engages in access tiering and secondly, when American end-users are accessing data repositories anywhere in the world via an American commercial ISP that again engages in access tiering.

The potential impact of the repeal on the iReceptor Plus project would thus increase as the number of non-academic repositories based in the US and the number of American end-users without access to an academic network would increase. This future potential impact cannot be

[25] Available at: https://crtc.gc.ca/eng/internet/berec.htm

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



predicted with enough accuracy, since it depends on the future success of the iReceptor Plus platform. Nevertheless, considering that currently, among the consortium partners, there are only two non-academic entities based in the US (namely Medgenome and 10X), the impact of the repeal of net neutrality rules in the US, at least from this perspective would be minimal.

In this context, it is also important to note that the repeal of net neutrality rules in the US does not imply that commercial ISPs will actually discriminate between data packets in practice. It is however impossible to predict with any accuracy whether and to what extent commercial American ISPs will engage in access tiering.

§2. Potential impact on data velocity

When the FCC in 2018 issued the 'Restoring Internet Freedom Order', it deleted several sections of the Code of Federal Regulations (CFR) which were installed by the 2015 'Open Internet Order' and related *inter alia* to blocking, throttling and paid prioritization practices of ISPs. According to these sections, internet access service providers should not:

- Block lawful content, applications, services, or non-harmful devices, subject to reasonable network management;[26]
- Impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management;[27]
- Engage in paid prioritization, meaning that the ISPs should not manage their broadband networks to directly or indirectly favour some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management in exchange for consideration (monetary or otherwise) from a third party, or to benefit an affiliated entity.[28]

Since these sections have been repealed, concerns have been raised that ISPs engaging in one of the above practices could lower internet speed of 'regular' data packets and as such increase the time span required for uploading and downloading data.

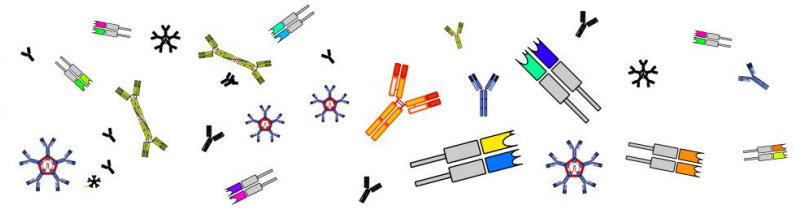
In the iReceptor Plus project, this would entail a risk of slower access to and use of the data available through the iReceptor Plus platform. However, given that the operations for big data

[26] Former Section 8.5, 47 CFR.

[27] Former Section 8.7, 47 CFR.

[28] Former section 8.9, 47 CFR.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)



analysis that will be performed by the iReceptor Plus platform are non-time critical this impact should be considered as rather small.

This assertation is strengthened by the fact that the potential slower access would be limited to a very small category of end-users, as explained in the previous section. Moreover, it is entirely feasible and non-hindering for end-users to run big data analysis operations at times when networks are less or not congested (e.g. in the night-time). Instant or high-speed performance is thus not a key specification or requirement for the iReceptor Plus platform and data visibility nor data use will be gravely hindered if broadband speed is somewhat slower.

Lastly, it should not be forgotten that under the 'Restoring Internet Freedom Order' ISPs are subject to a transparency obligation[29], which requires them to publicly disclose accurate information regarding the network management practices, performance characteristics, and commercial terms of the broadband internet access services, to enable consumers to make informed choices regarding the purchase and use of such services. This transparency rule allows iReceptor Plus partners running data repositories as well as end-users based in the US to verify if the minimum broadband speed levels guaranteed by a certain internet access service provider suffice for the efficient use of the platform.

§3. Potential impact on data security and privacy

Even though concerns surrounding the recent repeal of net neutrality rules under the Trump administration mainly relate to network performance, the question should also be raised if this departure from the net neutrality principle could also entail data security and privacy issues. In this perspective, it should be noted that, while the repeal of the 'Restoring Internet Freedom Order' does in itself raise concerns of data vulnerability or lack of data privacy, in 2017, the FCC also repealed the previous 'Broadband Consumer Privacy Rules'[30] installed under the Trump administration.

These rules, that required ISPs to protect the privacy of their customers, ensure greater transparency and strong security protections for personal information they collect, are thus no longer in place. Nevertheless, the privacy and security obligations amounting from the extraterritorial application of the General Data Protection Regulation (GDPR) will impose alternative guarantees in regards of data security and privacy.

[29] 47 CFR, section 8.1.

[30] US FCC, Report and Order, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services, WC Docket No. 16-106, 2 November 2016, available at: https://docs.fcc.gov/public/attachments/FCC-16-148A1.pdf

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)

D. Impact assessment and mitigating measures

From the above analysis, it appears that the foreseeable impact of the regulatory rollback in the US relating to net neutrality, will be rather low, if any at all. This conclusion is drawn from the

findings that (1) the repeal of net neutrality might be overturned in the near future, as a consequence of a bill introducing the '2019 Save the Internet Act' or the petition for review signed by attorneys-general from 22 states, (2) if the repeal of net neutrality is not overturned at the federal level, state legislation might still enforce the net neutrality principle, (3) the repeal can only potentially affect a small number of partners and end-users, given that only commercial ISPs (as opposed to academic ISPs) may abandon net neutrality, (4) the potential lowering of internet speed will not gravely hinder the visibility or use of data, since the big data analysis operations performed through the iReceptor platform are not time-critical and (5) any potential risk of data vulnerability or lack of data privacy is diminished by the extraterritorial application of the GDPR.

Nevertheless, the consortium would mitigate any remaining negative impact of the net neutrality repeal in the US. This could be achieved by relying on educational or research networks to the greatest extent possible, both when hosting and accessing the AIRR-seq data repositories. To this end, partners and end-users could make use of VPN-network or directly subscribe to academic networks where possible. If such solutions are not available, partners and end-users should rely only on commercial ISPs that provide sufficient guarantees with regard to data velocity, security and privacy.

This project is funded by the European Union's H2020 Research and Innovation Programme under Grant Agreement No. 825821 and Canadian Institutes of Health Research (CIHR)