2017 Internet access report - A/HRC/35/22

영장없는 통신자료제공

Requests for user data

18.Vague laws and regulations violate the legality requirement (see A/HRC/23/40,para. 50). The Communications and Multimedia Act of Malaysia, for example, permits authorities to order the disclosure of "any communication or class of communications" on "the occurrence of any public emergency or in the interest of public safety". The Act does not define the conditions that trigger a public emergency and certification by the King is deemed "conclusive proof on the point".33 In Qatar, law enforcement enjoys a broad right to seek access to providers' customer communications in cases of national security or emergency.34 These provisions empower authorities to request user data based on a mere assertion of national security. Users are thus unable to predict with reasonable certainty the circumstances under which their communications and associated data may be disclosed to authorities.

19.Providers should only be compelled to release user data when ordered by judicialauthorities certifying necessity and proportionality to achieve a legitimate objective. The Criminal Code of Canada requires law enforcement to submit requests for the disclosure of telephone records in criminal investigations to a judge for approval.35 In Portugal, the authorities must obtain a judicial order to compel the disclosure of communications data.36 However,

national law often exempts user data requests from judicial authorization. In Bangladesh, the authorities require only executive branch approval to access communications data belonging to telecommunications subscribers on the grounds of national security and public order.37

48 For example, all providers should vet user data requests for compliance with a minimum set of formalities, regardless of the origin of the request or the user affected. But while a multinational provider may have dedicated teams vetting requests, a small or medium-size provider may task its legal or public policy teams to perform the same function.

휴대폰실명제

20.Laws that require private actors to create large databases of user data accessible tothe government raise necessity and proportionality concerns. In Kazakhstan, telephone numbers, e-mail and Internet Protocol (IP) addresses and billing information must be stored by the provider for two years.38 The Russian Federation requires private actors to store the content of all their customers' calls and text messages for six months, and related communications metadata for three years.39 Both countries also require such data to be stored locally.40 In countries where mobile phones are a dominant means of communication, mandatory SIM card registration laws effectively require the majority of the population to divulge personally identifiable information (see A/HRC/29/32, para. 51).The mandatory retention of large amounts of user data

runs contrary to established due process standards, such as the need for individualized suspicion of wrongdoing.

SNI필터링

Undermining encryption

21.Since the Special Rapporteur's report on encryption and anonymity (A/HRC/29/32),unnecessary and disproportionate measures to undermine encryption have increased globally and threaten to undermine both the freedom of expression and digital security of users. In the United Kingdom of Great Britain and Northern Ireland, for example, the 2016 Investigatory Powers Act permits the Secretary of State to issue "technical capability notices" that require providers to remove "electronic protection" from communications — a measure that could compel backdoors or otherwise limit or weaken encryption.41 States have not provided sufficient evidence that such vulnerabilities are the least intrusive means of protecting national security and public order, particularly given the breadth and depth of other investigative tools at their disposal (Ibid., para. 39).

"온라인 수색"

22.Direct access to Internet and telecommunications networks enables authorities tointercept and monitor communications with limited legal scrutiny or accountability. Technological advances have enhanced the ability of law enforcement and intelligence agencies to obtain a direct connection to networks without the involvement or knowledge of the network operator.42

5G 네트워크슬라이싱

Paid prioritization

24.Under paid prioritization schemes, providers give preferential treatment to certaintypes of Internet traffic over others for payment or other commercial benefits. These schemes effectively create Internet fast lanes for content providers that can afford to pay extra and slow lanes for all others.46 This hierarchy of data undermines user choice. Users experience higher costs or lower quality of service when they attempt to access Internet content and applications in the slow lanes. At the same time, they may be compelled to engage with content that has been prioritized without their knowledge or input.

25.Several States prohibit paid prioritization. For example, the Netherlands, an earlyadopter of net neutrality, forbids providers from making "the price of the rates for Internet access services dependent on the services and applications which are offered or used via these services".47 The United States Federal Communications Commission 2015 Open Internet Order bans the "management of a broadband provider's network to directly or indirectly favour some traffic over other traffic ... in exchange for consideration (monetary or otherwise) from a third party, or to benefit an affiliated entity".48

. . .

33. A growing number of providers are establishing arrangements with media and other content-producing companies that threaten net neutrality and are lobbying

intensely for concessions on net neutrality standards. For example, as European regulators were developing net neutrality guidelines, 17 major providers in the region issued the "5G Manifesto", warning that "excessively prescriptive" guidelines would delay their investment in 5G, the next generation of mobile Internet connection.60

Access providers supply a public good

47. The digital access industry is in the business of digital expression; its commercial viability depends on users who seek, receive and impart information and ideas on the networks it builds and operates. Since privately owned networks are indispensable to the contemporary exercise of freedom of expression, their operators also assume critical social and public functions. The industry's decisions, whether in response to government demands or rooted in commercial interests, can directly impact freedom of expression and related human rights in both beneficial and detrimental ways.

자사 및 계열사 제로레이팅

28.. . .In contrast, the United States, followed later by the Body of European Regulators for Electronic Communications (BEREC), adopted guidelines involving a case-by-case approach.55 States that adopt a case-by-case approach should carefully scrutinize and, if necessary, reject arrangements that, among other things, zero-rate affiliated content, condition zero rating on payment or favour access to certain applications within a class of

similar applications (for example, zero rating certain music streaming services rather than all music streaming).

정보매개자 책임제한

49. . . .zealous enforcement of domestic law also poses human rights challenges in the digital access industry. For example, States may hold providers liable for, or otherwise pressure them to restrict, Internet content posted by users on their networks, under laws as varied as hate speech, defamation, cybercrime and lese-majesty. Yet such intermediary liability creates a strong incentive to censor: providers may find it safest not to challenge such regulation but to over-regulate content such that legitimate and lawful expression also ends up restricted.

14. Liability protections. From early in the digital age, many States adopted rules to protect intermediaries from liability for the content third parties publish on their platforms. The European Union e-commerce directive, for instance, establishes a legal regime to protect intermediaries from liability for content except when they go beyond their role as a "mere conduit", "cache" or "host" of information provided by users.31 Section 230 of the United States Communications Decency Act generally provides immunity for providers of "interactive computer service[s]" that host or publish information about others, but this has since been curtailed.32 The intermediary liability regime in Brazil requires a court order to restrict particular content,33 while the intermediary liability regime

in India establishes a “notice and takedown” process that involves the order of a court or similar adjudicative body.3
- **2018년 content moderation report A/HRC/38/35**

회사들의 의무 (예: 구글 2009년 유튜브 업로딩중단, 카카오 2016년 카톡감청중단, 페이스북 2018년 캐시서버 접속중단 행정소송)
68. Companies have an interest in operating in a legal environment that is human rights compliant, consistent due process and rule of law norms. Companies should explore all legal options for challenging requests that are excessively intrusive — such as requests for shutdowns of entire services or platforms, website takedowns that are clearly targeted at criticism or dissent or customer data requests that cover broadly unspecified users.111

[- **2018년 content moderation report A/HRC/38/35**]

가짜뉴스단속의무 (예: 2019 유튜브가짜뉴스차단법)
15. Imposition of company obligations.
Some States impose obligations on companies to restrict content under vague or complex legal criteria without prior judicial review and with the threat of harsh penalties. For example, the Chinese Cybersecurity Law of 2016 reinforces vague prohibitions against the spread of “false” information that disrupts “social or economic order”, national unity or national security; it also requires companies to monitor their networks and report violations to the authorities. 35 Failure to comply has reportedly led to heavy fines for the country’s biggest social media platforms.36

17. . . such rules involve risks to freedom of expression, putting significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability. **They also involve the delegation of regulatory functions to private actors that lack basic tools of accountability.** Demands for quick, automatic removals risk new forms of prior restraint that already threaten creative endeavours in the context of copyright. 40 Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic.41

회사투명성

23. . . The Global Network Initiative, a multi-stakeholder initiative that helps ICT companies navigate human rights challenges, has developed additional guidance on how to employ these tools.57 One tool of minimization is transparency: many companies report annually on the number of government requests they receive and execute per State. 58 However, companies do not consistently disclose sufficient information about how they respond to government requests, nor do they regularly report government requests made under terms of service.59

실명제 효용성

30. Real-name requirements. In order to deal with online abuse, some companies have “authentic identity”

requirements;89 others approach identity questions more flexibly.90 The effectiveness of real-name requirements as safeguards against online abuse is questionable.91 Indeed, strict insistence on real names has unmasked bloggers and activists using pseudonyms to protect themselves, exposing them to grave physical danger.92 It has also blocked the accounts of lesbian, gay, bisexual, transgender and queer users and activists, drag performers and users with non-English or unconventional names.93 Since online anonymity is often necessary for the physical safety of vulnerable users, human rights principles default to the protection of anonymity, subject only to limitations that would protect their identities.94 Narrowly crafted impersonation rules that limit the ability of users to portray another person in a confusing or deceptive manner may be a more proportionate means of protecting the identity, rights and reputations of other users.95

자율규제 기준

42. . . . . .when companies align their terms of service more closely with human rights law, States will find it harder to exploit them to censor content.

43. Human rights principles also enable companies to create an inclusive environment that accommodates the varied needs and interests of their users while establishing predictable and consistent baseline standards of behaviour. Amidst growing debate about whether companies exercise a combination of intermediary and editorial functions, human rights law expresses a promise to users that they can rely

on fundamental norms to protect their expression over and above what national law might curtail.124 Yet human rights law is not so inflexible or dogmatic that it requires companies to permit expression that would undermine the rights of others or the ability of States to protect legitimate national security or public order interests. Across a range of ills that may have more pronounced impact in digital space than they might offline — such as misogynist or homophobic harassment designed to silence women and sexual minorities, or incitement to violence of all sorts — human rights law would not deprive companies of tools. To the contrary, it would offer a globally recognized framework for designing those tools and a common vocabulary for explaining their nature, purpose and application to users and States.

. . .

45. Human rights by default. Terms of service should move away from a discretionary approach rooted in generic and self-serving "community" needs. Companies should instead adopt high-level policy commitments to maintain platforms for users to develop opinions, express themselves freely and access information of all kinds in a manner consistent with human rights law.

60. User autonomy. Companies have developed tools enabling users to shape their own online environments. This includes muting and blocking of other users or specific kinds of content. Similarly, platforms often permit users to create closed or private groups, moderated by users themselves. While content rules in closed groups

should be consistent with baseline human rights standards, platforms should encourage such affinity-based groups given their value in protecting opinion, expanding space for vulnerable communities and allowing the testing of controversial or unpopular ideas.

"기술적 조치"

67. States and intergovernmental organizations should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship.

행정심의 일반

68. States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression. They should avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users.

국가투명성

69. States should publish detailed transparency reports on all content-related requests issued to intermediaries and involve genuine public input in all regulatory considerations.