Internet as a subject of study in political science: technological, legal and organizational aspects

Current status of legal regulation of the use of the Internet: problems of global online identification

Michael YAKUSHEV

Security Issues in Cyberspace / MGIMO University / Moscow / November 2019
Identification online: some theoretical and practical issues

- Scope
- Terminology
- Anonymity on the Internet
- Identification: methods and practices
- Some conclusions
“On the Internet, nobody knows you’re a dog.”
Types of online identification system (Russian case)

1) Verified ID’s => according to the requirements of the federal laws
   - State-controlled/managed ID systems, banks, telecom operators etc.

2) Verified ID’s => outside any requirements of the federal laws
   - Car sharing, house sharing, marketplaces (freelance)

3) Non-verified ID’s
   - Social networks (accounts), e-Commerce, one-time e-mail addresses etc.

4) Other “me’s” (другой «Я»)
   - Online games accounts (nicknames), rating ID’s for e-Commerce or alike,
     “very personal’ (fictitious) ID’s for sensitive issues
Online Identification

- Identification (authentication, verification) of network users is caused by the need to ensure the stability of economy and public order.
  - Identification solves most cybersecurity issues.

- The Internet is the most important factor in socio-economic development (at the national level) and a key element of global stability.

- The identifiability (legal) of Web users, Internet service providers and owners of network resources is not a distinctive feature of the creation, operation and development of the Internet.
  - Due to the inherent historical reasons and technical principles of the Internet.

- There is no generally accepted understanding of how the issue of identification on the Internet can (should) be resolved, taking into account the cross-border nature of the Network and the degree of anonymity allowed there.
  - Standard identification procedures exist internationally only for WHOIS services in the DNS system (to be subsequently replaced soon).
  - The practice of regulation in different jurisdictions is not uniform.
Online Identification: key questions

- Is it possible to create a universal system for identifying Internet users, Internet service providers and network resource owners?

- If so, on what principles and using which international legal instruments?
  - What are the purposes of this identification?
  - How violations of the human rights should be prevented?

- If not, what are reasons?
  - Are “particular” (local, functional) identification systems possible?
- **Identification (1)** - establishing the identity of an unknown subject to a known one based on the coincidence of signs (marks, features, attributes)

- **Identification (2)** - the assignment of certain identifiers to objects and subjects [in information systems] and (or) comparison of the identifier with the list of assigned identifiers
  
  - “Name yourself to your information system”

- **Authentication** - verification of the identity of the subject presented by the identifier
  
  - Establishment of the correspondence (correlation) of the person with the identifier

- **Authorization** - granting a person rights to perform certain actions (or confirmation, verification of such rights)
  
  - Providing an identifiable person with certain opportunities in accordance with the rights laid down to him or checking the existence of such rights
Different identifies:

- **Human rights**
  - Name of the person (citizen) – legal capacity

- **Administrative relations**
  - Numbers and other identifying signs of identification documents of a citizen
  - Postal addresses

- **Intellectual property**
  - Commercial (and non-commercial) designations, trademarks, service marks, etc.

- **Property rights**
  - Property identifiers

- **Obligations (contract law)**
  - Domain names, email addresses, etc.

- **Technological identifiers**
  - IP addresses, digital objects identifiers

Different legal genesis
Anonymity in theory and practice

• Anonymous = «nameless»
  • Anonymity = human right (freedom)?

• Legal regimes of anonymity:
  • Anonymity is **permitted/allowed or implied**
  • Anonymity is **prescribed**
  • Anonymity is **prohibited/not allowed**
Relative anonymity: the real name is made known to only one counterparty, but remain unknown to others
  - Anonymous bank accounts (?), other professional secrets and confidential information (medical, audit etc.)
  - Telephone communication (subscribers numbers etc.)

Absolute anonymity: the real name is unknown to anyone (in general)
  - Users of payphones, Internet cafes, interactive communication on the Internet [use of web services that do not require registration]
  - Everyday ("offline") communication that does not generate legal rights and obligations

Passive and active anonymity
  - Anonymous person does not reveal his/her real name, “until asked” or
  - Anonymous person hides his/her name even if directly requested
Permitted (implied) anonymity

- **Most everyday situations** (бытовые ситуации)
  - Oral transactions/deals/agreements; simple contracts: city transportation, retail etc.

- **Intellectual property**
  - Copyright -> right to anonymous publication
    - Anonymity does not mean rejection of authorship!
  - Right to nickname (псевдоним)

- **The right of a journalist** to maintain the anonymity of his/her source of information (журналистская тайна)
Prescribed Anonymity

- Ethically determined privacy requirements, including bioethics
  - Adoption
  - Surrogacy
  - Treatment of HIV-infected persons etc.
  - Transplantation
- Personal data protection
  - Media information on persons, who have committed unlawful acts; victims
  - Anonymization of statistical personal information
- Voting
  - Inadmissibility of identifying completed ballots => with specific voters
    - Not only for public officials!
When anonymity is NOT allowed (prohibited)

- Possession of [real estate] property, strict (tort) liability (источники повышенной опасности)
  - “nameless” property => res nullius (nobody’s thing)
- Criminal liability (уголовная ответственность)
  - Identification of the individual (entity) is mandatory to hold someone liable
  - Not to be confused with the compensation for harm/damage from unlawful acts [insurance coverage of risks from damage caused by an anonymous and/or unidentified person => is possible]
- Any other legally significant actions, where the personality of the subject matters
Online Anonymity (1)

- IP-addresses
  - Including addresses of the users who submit web search queries
  - Are the IP-addresses «personal data»?

- «WHOIS» Service
  - Collisions with European GDPR

- Anonymous (=pseudonymous) e-mail addresses, including free online e-mail services

- Use of cryptography for protection of information; “anonymizers”, VPN’s and similar software tools

- Legal Interception (COPM) and effectiveness of measures of telecom operators requested by law-enforcement agencies
  - Telegram case (Russia, 2018)
WHOIS service
Online Anonymity (2)

- **Proportionality** of restrictions on rights and freedoms, guaranteed by basic legal acts
  - Correlation with "off-line" types of communications (a postal letter/envelope may be sent by an anonymous sender; the contents of the letter is protected by secrecy of correspondence rules)

- Existence and applicability of the **government strategy** for usage of cyberspace
  - (Doubtful in case of the Russian Federation 😕)

- General approach: what is prohibited off-line => should be prohibited on-line; to prohibit something on-line in the absence of off-line restrictions, **VERY** substantial legal grounds are needed
  - The right to anonymity => Article 8 of the European Convention on Human Rights [private and family life]

- **Declaration on the Freedom of Communication on the Internet** (adopted by the Committee of Ministers of the Council of Europe on May 28, 2003) on ensuring anonymity:
  - In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member States should respect the will of users of the Internet not to disclose their identity. This does not prevent member States from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.
Online Anonymity (3)

- Ability to use anonymity for illegal (antisocial) purposes
  - Illegal receipt of information (intellectual property) by anonymous users
  - Distribution of illegal information (not intended for children etc.), or malicious software
  - Terrorism (influencing public opinion, creating panic, spreading rumors, etc.)

- Limitations of anonymity
  - Stop violation of the rights of third parties (it is necessary to protect not only the rights of anonymous users, but also the legal rights of third parties)
  - Exempt the liability of owners of Internet services that allow their use anonymously

- An Internet user has the right to know what rights he has, what responsibilities he bears, what restrictions and under what circumstances may arise
  - See terms of use, user agreements etc.
Methods of identification

- **ID documents**: prescribed by legislation (passport, abstract from the Register(s) + set of *applicable procedures* for legal entities), *other* methods of “conditional identification” (accounts in social networks, verified by friends and followers);

- **Authentication**: login + password, electronic certificates (digital signatures), hardware equipment (smart access cards, USB sticks/identifiers [may require readers]), unique identifiers (bank cards, social security numbers, pension registry egnumbers, tax numbers, biometrics (fingerprints, face photos), [corporate] verified email address, network/subscribers identifiers (phone numbers, IP addresses, domain names, accounts in social networks and services), + (...)
Automatic tracking of users’ online activities

• Each time you connect to the Internet
  • You specify a unique identifier (login) and (or), you may identified in many other ways (IP address, dial-up connection telephone number, subscriber number of the agreement with the access provider, etc.)

• Each time you visit a resource on the Internet
  • The following information may be recorded (the list is not full):
    • The network address of the page you are viewing (URL)
    • The network address of the referring page
    • User IP address (provider and country of incorporation)
    • Browser specifications (type, language, built-in extensions, application support) and other computer settings (screen resolution, colors)
    • Proxy data
    • Cookie and Java Support
    • Time Zone

• (...)

Each time you connect to the Internet:
- You specify a unique identifier (login) and (or), you may be identified in many other ways (IP address, dial-up connection telephone number, subscriber number of the agreement with the access provider, etc.).

Each time you visit a resource on the Internet:
- The following information may be recorded (the list is not full):
  - The network address of the page you are viewing (URL)
  - The network address of the referring page
  - User IP address (provider and country of incorporation)
  - Browser specifications (type, language, built-in extensions, application support) and other computer settings (screen resolution, colors)
  - Proxy data
  - Cookie and Java Support
  - Time Zone
Complex (combined) methods

- **Multifactor identification** [some social networks, domain name registration in Russia]: providing information about yourself by the applicant + indicating a mobile phone number for subsequent authorization, {intermediate options are possible}
  - The need to use only the telephone number of a given country
- [some social networks and services]: “implied”, “friendly” **authentication** (recognition as a “friend”), as well as additional verified status for individual accounts; the expanding practice of using Open-ID
  - Absolute reliability is not guaranteed (operator of a social network as an intermediary)
- [separate services]: providing a **scanned copy of identifying documents** (passports)
  - High probability of fraud
  - The difficulty of processing personal data under the laws of Russia
- [Russian public services portal, initial version]: “degenerate case” with sending authorizing notifications (passwords) by regular mail, at the beginning of the service
Different legal status:
- Provided by different organizations (regional registries, global and local registrars)
- There is no (as a rule) “comprehensive” national regulation
- At the global level, only technical regulation exists (RFP, RFC)

Unresolved issues:
- Correlation with off-line identifiers (postal addresses, P.O.Boxes)
- Verification data from WHOIS and further development (new protocols)
- Domain name as an example of uncertainty
  - Intellectual property (means of individualization)
  - Confirmation of the existence of a contractual relationship (legitimation mark)
  - Identifier similar to the mailing address
  - The analogue of "network real estate object" (domain)
Some conclusions.

- No simple solutions are visible
- Different national laws make identification systems efficient only inside national territories
- International agreement (universal convention) on global identification is possible in theory; in practice it requires the depoliticization of the problem
  - Technological neutrality principle should be followed
  - Cross-border conflicts should be avoided (prevented)
- Anonymity is one of natural human rights (part of the privacy rules), and, as such, it should be respected.
  - Anonymity should not be used to violate human rights of the third parties (other people with lawful behavior)
- Off-line freedoms and rights should not be restricted online
  - Same balance with the online identification systems vs. off-line documents
Thanks for your attention!