Alternative internet(s): the benefits and challenges of distributed services

In our series on alternative internet(s), Melanie Dulong de Rosnay, researcher at the French National Centre for Scientific Research (CNRS) Institute for Communication Sciences and a visiting fellow at the LSE, looks at the benefits and challenges of distributed internet architectures, including difficulties in assigning responsibility, liability, and identity. Read the introduction to the series that explains more about alternative internet(s) here.

Activists are relying on alternative applications to protect their communication privacy from governments and corporations. From anonymity software, like Tor, to local mesh messaging in absence of a connection, like Firechat, distributed architectures for online tools provide alternatives to centralised services which can be tapped, controlled or shut down by central authorities. Used in conjunction with encryption, these tools are helping demonstrators, activists, journalists and dissidents to circumvent surveillance and address asymmetries of power with repressive regimes or intelligence agencies.

But such distributed services can also be used for more practical and less political reasons. Mesh or community wireless networks offer an alternative communication infrastructure to ensure resilient access to the internet in rural areas, at festivals, after disasters, or in emergency situations. Besides, these grassroots initiatives are providing an alternative to expensive or unavailable commercial ISPs. In that sense, they constitute local commons-based peer production of connectivity.

However, alternative distributed services are also facilitating the dissimulation of criminal activities, leading to the creation of darknets such as Silkroad, which was recently taken down by the FBI and resurrected a few days later.

Data fragmentation and encryption

Liability for law infringement or for facilitating cybercrime can be determined only if authors can be identified and found guilty. The law usually allocates tort to individual persons found responsible, rather than to unstable groups of peers. Peers whose devices are part of an alternative network are often unaware of the content they are incidentally helping to circulate by providing a bit of the infrastructure of the service of hosting, connection or browsing. With community wireless relying on a distributed architecture, users are not monitoring or storing connection metadata or content exchanged. With distributed storage, as an alternative to cloud storage that carries risks of hacking, data is fragmented, locally encrypted, then distributed among the hard drives of users linked in a distributed network architecture. Peers are not identified by a central authority, only the final peer reconstructs the full file, and neither users nor developers of the service, nor the police, can control or filter the files.

Regulatory answers

Currently it is not possible to know whether a peer is helping an activist or a cybercriminal to remain anonymous. Legal and judicial options are limited. Node owners cannot be held liable for infringement if they benefit from Internet Service Providers' safe harbour from liability as intermediaries as devised in the EU and the US. No procedure of notice-and-take down could apply if the content is not made public.

It could become illegal to share a connection. Judicial proceedings for negligence to secure wireless connections have been practiced both in France with three strikes laws and in the US with police raids. However, the identification of the IP address of a device, which is dynamically changing over time, can be changed or faked, and thus cannot be held as a proof identifying a person.

Legislation could also outlaw distributed applications. Between 2007 and 2011, Italy required Internet Service Providers to identify users, which *de facto* forbade open wifi without registration. Vivendi Universal tried to make p2p filesharing software illegal in France in 2006 during the implementation of the European Union Copyright Directive, but the proposed amendment was rejected because p2p can be used for legal purposes. Such regulatory responses have a chilling effect on freedom of expression and legitimate usages of innovative alternative technologies.

Liability immunity, social responsibility and commons-based policing

The peer production of alternative internets also contributes to improving quality of service and optimising resources. Even though the role of each peer is not crucial from a legal point of view, they all carry a social responsibility because their collaboration guarantees the system will effectively function.

Trying to distribute the liability as an answer to the legal challenge raised by distributed architecture could also mean monitoring, reporting and sanctioning illegal uses, following Elinor Ostrom's Design Principles numbers 4 and 5. But surveillance crowdsourcing can take place only in services and communities which present a certain degree of centralisation: Diaspora, the semi-distributed social network, may for instance contact nodes or administrators hosting ISIS propaganda. But if crime cannot be seen or allocated to a person due to encryption and fragmentation, it is unlikely that a collective sense of responsibility will develop. Besides, collaborative policing without checks and balances could lead to the exclusion or the discrimination of users based on their IP address or for other illegitimate, disproportionate reasons.

Access to the technology

Even if technical efforts required to set up or join some alternatives, as opposed to the ease of installation of commercial counterparts, may prevent their take-off, alternative internets contribute to emancipation and autonomy through technology. They constitute a valid alternative to the lack of security, privacy and sustainability of private service providers. If they are really effective in preserving privacy, they also offer a solution to the lack of regulation against decision-making based on data mining. Some are less convenient to use than the commercial services and products. Some user interfaces also entail a learning and implementation curve, or require the joint usage of complex anonymisation software, which might lead to exclusion of the less digitally skilled. But encryption, once considered an alternative, is becoming mainstream when popular applications such as Whatsapp are embedding it by default. In other words, we may be heading towards a world where alternative internet structures and tools become the norm.

This article gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics.

November 26th, 2014 | Alternative Internet(s), Featured, Guest Blog, Internet Freedom, Privacy | 0 Comments