ITU EXPLAINERS
DIGITAL OBJECT ARCHITECTURE

What is Digital Object Architecture?

Digital Object Architecture (or DOA) is a way of managing digital information in a network environment. At present, online digital information is managed through the internet architecture which focuses on 'hosts' (the systems that are connected to the internet, such as computers and servers) and the connections and transmission of information between them. DOA uses an alternative architecture which instead focuses on the discovery and delivery of information in the form of 'digital objects'.

A digital object is a structured record which contains data (such as a text file, sound recording, image, photograph, video or some other piece of information), information about that data (such as restrictions on access to the digital object, information about ownership and identifiers for licensing agreements, if appropriate) and metadata (such as when it was created).

Under the DOA system, each digital object has a unique and permanent digital object identifier (DOI) which is independent of the underlying physical system. A good analogy is the way that books are currently tagged with ISBN numbers. If you provide an ISBN number to a librarian, or enter it into a search engine, you will be able to quickly identify and locate that book. Similarly, if all digital objects were given a DOI, you would be able to use that DOI to discover and locate that object. The DOI would even include information about the specific computer, server or other device the digital object was being hosted on.

The DOA system has a number of advantages over the current system, which relies on web addresses (and the underlying IP addresses). For example, in the current system, links to files online can break when websites and web addresses are modified, making the data inaccessible. This would not happen in a DOA system, because DOIs are permanent. And while information online in the current system does not necessarily tell you everything you want to know about it (such as what restrictions there are on its use, or who owns it), the DOI would also contain this additional information.

Why is DOA being discussed at the ITU?

While, originally, DOA allowed for different possible resolution systems (the systems for labelling each digital object) to be defined and used, over time it has become almost exclusively tied to one system, called the Handle System. The Handle System gives people a means of finding the location of a digital object using its DOI. It uses a hierarchical model, with a Global Handle Registry (GHR) at the root and Local Handle Services under the root. Each Local Handle Service can also contain its own hierarchy of Handle Services.

For the first 20 years or so of the Handle System, the root GHR was an organisation called the Corporation for National Research Initiatives (CNRI), set up by Bob Kahn. However, in 2015 this role was handed over to a body called the DONA Foundation. The DONA Foundation was established in 2014 with the support of the ITU who worked with the CNRI through Memoranda of Understanding to develop plans for the transition. After its founding, the DONA Foundation signed a Memorandum of Understanding with the ITU in which the ITU agreed to provide secretariat support to the DONA Foundation, to accept and hold the intellectual property rights and licences on GHR technology and software from the DONA Foundation, and to provide guidance to the DONA Foundation on matters of public policy. In addition to operations of the GHR, the DONA Foundation agreed to contribute its intellectual property rights to the ITU and to submit issues related to public policy to the ITU.

The Handle System has been operated for the last 20 or so years mainly for specialised use in digital libraries, and for research . However, some countries are now trying to have DOA adopted as the global standard managing 'internet of things' (IoT) devices, and proposing that the ITU be the sole entity authorised to administer the DOA's GHR, through the DONA Foundation.

Why should human rights defenders care?

The adoption of DOA, under the administration of the ITU, could adversely impact a number of human rights, particularly the rights to privacy and freedom of expression:

Privacy: DOA potentially provides the ability for governments (or other non-state actors) to track all files and other pieces of information with a DOI within their borders, with the further possibility of tracking which devices and individuals access them. For a government (or any other actor) to have access

to all the information that a person was searching for and receiving would represent a serious invasion of their privacy, particularly if such information was personal or sensitive, e.g. information relating to sexual orientation and gender identity, to HIV or other health status, or to particular political or religious beliefs. In societies where certain groups face discrimination, persecution and violence, information which identified an individual as belonging to a particular group or identity (such as the LGBT community, a religious minority, or a political party or movement) could put their security at risk.

Freedom of expression: Because all online information would be allocated a DOI, any DOA system which gave governments control over national Handle Services, for example, would enable a government that wished to restrict access to certain online content (e.g. information critical of the government, or relating to issues which are controversial in some parts of the world, like LGBT rights or abortion) to be able to block access to the respective DOIs within their borders.

Where is the discussion taking place?

Current discussions around DOA are primarily taking place in ITU-T Study Group 17 (Security). However, the issue of DOA has been raised previously in other forums within the ITU. In 2016, for example, at the World Telecommunication Standardization Assembly, several states put forward proposals for further research into DOA. All were ultimately rejected, save for one which added an oblique reference to DOA into a new resolution on combatting counterfeit telecommunications and ICT devices.

It is likely that further discussions around DOA will take place at upcoming ITU forums and events, including the World Telecommunication Development Conference in October 2017 and the Plenipotentiary Conference in late 2018.