UTS ePRESS

Cultural Studies Review

Vol. 25, No. 2
December 2019

CULTURE REVIEW

Cookie

John Frow
University of Sydney

Corresponding author: John Frow: john.frow@sydney.edu.au

DOI: https://doi.org/10.5130/csr.v25i2.6899
Article history: Accepted 1/11/2019; Published 22/11/2019

Cookies are randomly generated strings of numbers and letters that can be sent from a website to a user's browser, where they are stored in a subdirectory on the computer for the length of a session and returned unchanged to the website; their role is to identify and remember the computer and thus provide continuity between visits to and transactions on that site. The HTTP cookie was initially developed by Netscape in 1994 to authenticate the account with which the website was dealing and to record a browsing history. Because it introduces memory, or statefulness, into a stateless system such as the basic internet protocols, which retain no memory of previous interactions, it can recall those interactions through the assignment of a unique visitor ID. That makes it possible to construct a shopping cart of items, for example, or to fill in an online form, rather than having to start anew with each item, or to remember login details and preferences, or to resume interaction on a site on a user's subsequent visit, or to collect information about their buying habits. By recording and retrieving state information (information about a set of conditions at a moment in time), cookies are, we might say, deictically charged: localised in time and space to a particular Internet subject.

On most browsers, tracking cookies can be disabled or deleted by users in order to defend their privacy. That privacy—that store of detailed personal information—is, however, the primary commodity on the web for information brokers and the advertisers who buy from them. In response to the threat of deletion, in 2005 an American advertising company rejoicing in the name United Virtualities developed a backup system for cookies known as Flash cookies, which, like HTTP or tracking cookies, render a browsing activity stateful.[1] Flash cookies are tracking devices within the 'local shared objects' area of Adobe Flash, which is installed on almost all computers, and its key features are that it is *persistent* (it doesn't have an expiration date) and that it is a *zombie cookie*, with the ability to recreate or 'respawn' a deleted tracking cookie using data stored in Flash. It is hard to eradicate, it is set not to ask the user's permission to store data, and it is used to collate 'ostensibly nonpersonal behavioral information in order to produce a closely approximate demographic portrait including age,

Citation: Frow, J. 2019. Cookie. *Cultural Studies Review*, 25:2, 208-210. https://doi.org/10.5130/csr.v25i2.6899

ISSN 1837-8692 | Published by UTS ePRESS | https://epress.lib.uts.edu.au/journals/index.php/csrj

DECLARATION OF CONFLICTING INTEREST The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article. **FUNDING** The author(s) received no financial support for the research, authorship, and/or publication of this article.

gender, location, educational level, income, consumption habits (purchasing and reading), sexual preference, and health issues'.[2]

A range of other tracking devices supplement the work of local shared objects or Flash cookies. On mobile phones, where cookies are relatively inefficient because they must be reset when a browser is closed and they can't be shared between apps or devices, they have a more limited existence. A range of alternative methods of tracking are currently being developed, including Client/Device Generated Identifier, Statistical ID, HTML5 Cookie Tracking, and Universal Login Tracking. On computer web browsers, third party cookies which are placed on a user's computer by a web site with a domain name other than the one being visited—in banner ads displayed on a website, for example—enable tracking of users across websites, and the cross-synchronisation or cookie-matching of different identifiers assigned to users allows the creation of a unified identifier which can then potentially be correlated with an offline identity, or rather, with the datasets assigned to it.[3]

Even harder to detect than Flash cookies, web beacons (also known as web bugs, pixel tags or clear gifs) were originally single-pixel .gif tags in a web document or an email, often of the same colour as the background and so completely invisible; opening the page or email triggers a request from the computer to the remote server, thus sending identifying and tracking information about the computer. Later versions of the web beacon use other pictorial or non-pictorial elements such as banners or buttons, or the HTML frame, which may be independent of the framed content—an advertisement, for example—and sends identifying information to the third-party server that owns it. Beacons can thus 'track user interaction on the page, including typed entries and mouse movements', and use this information to follow movements across the Internet. They 'may also be used to retrieve files stored on a hard drive, record conversations through a computer microphone, or transmit images from a computer's video camera',[4] as well as collecting a range of personal information and sending it on to advertising profilers.

The collection processes employed by cookies and cognate devices are structurally homologous with those of state intelligence services. What Shoshana Zuboff calls 'online surveillance at scale'[5] harvests information that had never previously been captured—'about people's time-space paths through the course of the day, the details of when and where they chat with friends, even the random queries that drift through their minds (to the extent that these are transformed into Google searches)'[6]—and it does so by making use of algorithmic procedures, such as mathematical association rules, which moved from the commercial sphere where they were initially developed to that of national security apparatuses.[7] But the ubiquity of commercial and state surveillance doesn't mean that we live in a world of totalised panoptic control. Mark Andrejevic has suggested the alternative metaphor of a world made up of a series of distinct but sometimes overlapping digital enclosures, meaning the coverage range created by the interactive and data storage capabilities of any digital surveillance technology: a world characterised, then, 'by a proliferation of different monitoring networks with varying capabilities for information capture under the control of different entities'.[8] Under certain conditions (a totalitarian government with a tight hand on the public domain, for example) data from a number of different enclosures might be aggregated; and security agencies such as the NSA do in practice make use of commercially gathered data, either by stealing it or by exploiting software vulnerabilities or merely by requesting access to it. This is an area in which the tech companies are pushing back, but probably the most we can say about this is that the balance between privacy and security is precarious and in a state of considerable flux. Further, the coexistence of digital enclosures within an overarching assemblage means

that information collected for commercial purposes might be migrated 'across a range of other, sometimes unanticipated functions'.[9] The trade goes both ways, with technologies and software developed for military or security purposes finding their way into the surveillance activities of business—or, more precisely perhaps, with an increasing lack of differentiation between these spheres.

Endnotes

1. Janice Sipior, Burke Ward and Ruben Mendoza, 'Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons', *Journal of Internet Commerce*, 10: 1 (2011), p. 3.

2. Rita Raley, 'Dataveillance and Countervailance', in *"Raw Data" is an Oxymoron*, ed. Lisa Gitelman (Cambridge MA: MIT Press, 2014), p. 121.

3. José Estrada-Jiménez, Javier Parra-Arnau, Ana Rodríguez-Hoyos, and Jordi Forné, 'Online Advertising: Analysis of Privacy Threats and Protection Approaches', *Computer Communications* 100 (2017), p. 38.

4. Sipior et al., p. 5.

5. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019), p. 83.

6. Mark Andrejevic, 'Ubiquitous Surveillance', *Routledge Handbook of Surveillance Studies*, ed. Kirstie Ball, Kevin D. Haggerty and David Lyon (London: Routledge, 2012), p. 93.

7. Louise Amoore, 'Governing by Identity', *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, ed. Colin J. Bennett and David Lyon (London: Routledge, 2008), p. 26.

8. Andrejevic, p. 93.

9. Ibid., p. 94; cf. David Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique', *Big Data and Society* (July – December 2014), pp. 5-6, 8.