City Research Online

City, University of London Institutional Repository

This is the accepted version of the paper.

This version of the publication may differ from the final published version.

Title: Cookies – More than meets the eye

Author: Elinor Carmi, Goldsmiths, University of London, UK.

In the last episode of Halt and Catch Fire's third season, AMC's television series about the tech industry in the 1980s, we see the protagonists argue about the future of the World Wide Web. The year is 1990. Joe MacMillan, the 'Steve Jobs' ego-maniac-visionary of the series, suggests that "the moment we decide what the web is we've lost. If we try to tell people what to do with it – we've lost. All we have to do is build a door. And let them inside". But MacMillan's character was wrong. We have been told how to use and think about the web for decades and some of it starts with the very basic elements of the web-cookies.

Although web-cookies have revolutionised the way we use and understand the web, very little has been written on them. In fact, most research and articles on web-cookies, which come mostly from computer scientists, say the same thing – they are 'just' text files sent from a website and stored on someone's computer. Computer scientists call cookies a 'state' (Kristol and Montulli, 1997) which means a form of memory. Cookies revolutionised the web because instead of treating each time you use the web as a 'new' and importantly – *anonymous* – session, it began to remember what you did previously. Cookies gave the web a memory; it gave your actions on the web a 'past', a past which you have no idea about or access to. But such framing of cookies is only one way of looking at it. And looking at it has been quite hard because they are not visible to us. Adopting computer scientists' views has lead to very limited understanding of various media and communication phenomena. Believing that cookies are mere technical and non interesting stuff has limited our ability to see beyond such arguments. What I am trying to say is that actually, we have been looking at cookies wrong all this time.

These limitations often come from disciplinary boundaries. Many digital phenomena challenge researchers because they cannot neatly fit into their discipline. Disciplines have been disciplining us to think and conduct research through particular lenses about our research objects. But what many digital phenomena show us is that we have to start looking at them differently, we have to look beyond the hype. To do that means getting outside of your comfort zone and start using theories and methods from other disciplines. It means customising your research by taking elements from different theories and methods and weaving together a new assemblage to understand how things like software, protocols, codes, algorithms and also, of course, cookies work. Importantly, just because these media phenomena have been developed by computer scientists and engineers does not mean we need to automatically accept their definitions and ways of thinking about them.

The same kind of computer science assumptions occur when you try and research spam. When trying to look beyond Nigerian Princes and Monty Python (excellent) sketch media and communications scholars are usually lead to believe it is about those 'evil' internet things. But what *is* spam, really? Is it an object? Is it a protocol? Is it a feature? Is it a culture? What is it? It appears that with these digital phenomena, we were meant to believe one is tasty and necessary, whilst the other is disgusting and should be made junk. But how exactly?

Eat this! Spam and cookies

Since law and computing need specific definitions to operate (and execute), these fields are extremely productive for digital phenomena. Both of these fields also present their definitions as objective truths, hiding the politics, struggles and power structures (which include lobbying of influential media players) engineered into their discourses. Such discourses, then, should not be taken at face value, but rather should be peeled carefully one next to the other along with other data. When looking at legal discourses about spam, one finds two main arguments – that is unsolicited and that it is bulk communication. However, as I have recently showed (Carmi, 2017), both of these claims are wrong, and have been constructed as such to legitimise similar practices - cookies.

The end of the 1990s and beginning of the 2000s was a transitional period for the internet that went from a subscription business model to free content that we have come to know today. But as you already know, nothing comes for free. And the way that the internet was funded was by trading with people's data, the new currency. This was made possible by strong lobbying of the advertising industry of legal systems and internet standard organisations such as the Internet Engineering Task Force (IETF). The main lobbying, however, was on people's perception of media phenomena, mainly that cookies are just text files sent from publishers or advertising networks to people's computers. But looking closely at the ingredients, it seems that cookies are, in fact, a form of communication. Cookies communicate between your computer and advertisers while the message is *you*, or more accurately - people's behaviours. This 'message' helps build people's profiles and then tailor advertisements for them which is how the internet has been funded from the beginning of the 2000s until today.

Most of the research presented by legislators and others about spam indicates how much it costs to the users and the operators (for example internet service providers). But the same question was never asked when it came to cookies. Cookies managed to avoid creating a burden on the internet infrastructure with special browser design. Interestingly, there is no research into how much bandwidth the cookies communication cost people, but with current debates about ad blockers it is clear that both cookies and other forms of online advertising do cost people in terms of bandwidth. Only lately, since the introduction of adblockers which emerged from

around 2005, people experience the web differently and some people started to ask these questions. According to Rob Leathern (2016), for example, ads cost people $8 billion. So cookies cost us, even more than just bandwidth, but all we are left to do, at least in Europe, is press 'I agree/consent/OK'. Many publishers, websites and platforms do not allow people to access their services without allowing cookies to communicate with their computers. By doing so, we are turned into a captive audience being told that it is either their (cookies) way or no internet highway.

Influenced by the advertising industry lobbying, the European Union legislation legitimised cookies by saying that they are valuable for funding the internet. As the e-Privacy Directive from 2002 says: "so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising" (2002/58/EC, Recital 25). But if they are so important to funding the internet, why are they hidden? Well, if browsers, publishers and advertising companies would follow the IETF cookie standard cookies would be visible. The IETF standard of cookies recommend for a visual display of the 'back-end' to show people the cookie communication happening on their computers. Imagine that the visualisation tools we have now, such as the Electronic Frontier Foundation (EFF)'s Privacy Badger, Firefox's Lightbeam or Baycloud would be browsers' default visual display. This means that we might have had split screens where we could see what is happening to our computers, and not only cookies, but other operations. We could have seen exactly how bulk the cookie communication is (because publishers and advertising companies send dozens if not hundreds of cookies), how it actually tastes like spam.

Such moves have political, social and economical implications about the way that the web functions. It influences the way we experience and understand the web. It means that we could have had much more control, knowledge and choice to interact with our computers and others differently. Importantly, it would challenge the power relations between various intermediaries such as publishers, media platforms, browsers and advertising companies and people who use the web. People would start asking questions that start to emerge today about what happens to their data, how is it being traded, by whom and for what purposes? If we, our data selves, are the currency that funds the internet, then we need to understand what is the cost. What it also shows, is how important it is for scholars to examine, question and challenge 'common-sense' arguments about what seems to be 'not interesting', 'boring' and 'technical' media phenomena. Don't eat everything that computer scientists feed you.

References

Carmi, Elinor (2017) Regulating behaviours on the European Union internet, the case of spam versus cookies. International Review of Law, Computers & Technology. Epub ahead of print 20 March 2017. DOI: 10.1080/13600869.2017.1304616.

Directive on privacy and electronic communications (e-Privacy) (2002/58/EC).

Available at: http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

Kristol, David M and Montulli, Lou (1997) RFC 2109 - HTTP state management mechanism. IETF. Available at: https://www.ietf.org/rfc/rfc2109.txt (accessed 22 July 2017).

Leathern, Ron (2016) Shitty ads cost iPhone users $8 billion a year (just in the US)… why aren't you blocking ads already?. Medium. Available at: https://medium.com/@robleathern/shitty-ads-cost-iphone-users-8-billion-a-year-5a67c6f43097 (accessed 22 July 2017).