The Cancer of the Internet

Author : James Grimmelmann

Date : November 12, 2013

Finn Brunton, [Spam: A Shadow History of the Internet](#) (MIT Press, 2013).

Technologies do not come with social or legal instruction manuals. There is nothing inherent in rooftop strobe light bars to suggest that police may use them but not civilians, or in thermal imaging cameras to suggest the reverse. The public must figure out what to do with each technology as it becomes available: embrace, ignore, regulate, ban. If we are lucky, the rules distinguishing acceptable from forbidden uses can come, over time, to seem like natural features of the technology itself. But they are not: the rules have to come from somewhere, and someone had to work them out, somehow.

For an example, consider today's debates on what to do about drones. Or for another, consider spam, the subject of Finn Brunton's erudite and entertaining *Spam: A Shadow History of the Internet*. Brunton pushes his history far back before the 1994 advertisement from a pair of immigration lawyers that is usually thought of as spam's Ground Zero. He notes, for example, a 1971 antiwar message sent to every user of the Compatible Time-Sharing System and a 1978 announcement of a DEC computer demonstration sent to all West Coast ARPANET users–both of which provoked debate around the acceptable boundaries of network use. Brunton argues that well into the 1990s, spamming was considered a primarily social offense, separate and distinct from commercial self-promotion, and of an entirely lesser order than "net abuse" (P. 39) like crashing computers. Spam was a form of free speech, and like other inappropriate speech was to be met with censure rather than censorship.

But this attitude changed, and changed sharply, as the first wave of commercial spammers arrived en masse. Unlike the earlier "spammers," who could be telephoned and reasoned with, or shamed into silence, or simply identified and ignored by users' personal message filters, these new operators both flaunted their identity as outsiders to close-knit online communities and aggressively covered their tracks to keep the messages getting through. In the face of these new actors, Brunton shows that spam was effectively redefined as a legal and technical problem rather than a social one. To many antispam activists, the great danger of CAN-SPAM was that it would legitimize spam. But the combination of a legislative framework with reasonably effective filtering had another effect entirely–it "destroyed email spam as a reputable business model," (P. 143) and "eliminated the mere profit-seeking carpetbaggers and left the business to the criminals." (P. 144)

Spam is thoughtful about the ontology of its namesake. We are accustomed to thinking of spam as an email phenomenon. But, as Brunton effectively demonstrates, email spam is only one instance of a much larger pattern. Today there are Facebook spam, LinkedIn spam, blog comment spam, Twitter spam–and many more. Indeed, spam's contested definitions create any number of difficult boundary cases. Gmail's inbox tabs shunt "Promotions" into a separate folder, even when the recipients have affirmatively opted into receiving these emails. Or, to take one of Brunton's examples, Demand Media "commissions content from human writers (who are willing to meet very low standards for very little money) on the basis of an algorithm that determines ad revenue over the lifetime of any given article." (P. 162)

Brunton's own definition of spam, offered at the end of the picaresque tour, is "the use of information technology infrastructure to exploit existing aggregations of human attention." (P. 199) Both halves are

exactly on point. Spam is medium- and technology- agnostic, but it is inherently a technological phenomenon: without the amplifying power of commodity copying, spam's characteristic bulk is impossible. And spam is essentially a problem of attention hijacking: the systematic conscription of large and diffuse audiences by abusive speakers.

Much of Brunton's story of spam is told through the eyes of its enemies, from the vigilantes who made tried to burn out commercial spammers' fax machines to the modern programmers who build increasingly complex filters to identify and delete spam. Significantly, this is history through the eyes of its losers: the story of the tide as related by King Canute. Brunton conveys effectively the sheer frustration felt by anti-spam activists. The network they loved was being abused by outsiders who pointedly rejected their values, but they found themselves unable to stop the abuse. One countermeasure after another fell before the onslaught: killfiles, cancelbots, keyword filters, blackhole lists, and so many others.

Roughly the second half of the book is devoted to the remarkable technical evolution of computer-generated spam. Brunton traces the rise of keyword stuffing, hidden text, Oulipo-esque email generators, spam blogs, content farms, Mechanical Turk-fueled social spam, CAPTCHA crackers, Craigslist bots, malware as a source of spam, and online mercenaries renting out botnets to the highest bidder. This escalation–from a pair of immigration lawyers in over their heads to a "criminal infrastructure" industry (P. 195) in less than two decades–is nothing short of alarming.

Spam is also one of the most nuanced books to unpack what makes the postmodern post-Web 2.0 Internet tick. Borrowing Matt Jones's concept of "robot-readable" media–"objects meant primarily for the attention of other objects" (Pp. 110-11)–Brunton gives an insightful metaphor of the uneasy coexistence of human and software readers online:

> Consider a flower–say, a common marsh marigold, *Caltha palustris*. A human sees a delightful bloom, a solid and shiny yellow … A bee, meanwhile, sees something very different: the yellow is merely the edging around a deep splash of violet invisible to human eyes–a color out on the ultraviolet end of the spectrum known as "bee violet." It's a target meant for the creature that can fly into the flower and gather pollen. The marsh marigold exists in two worlds at once. (P. 110)

The visible language of QR codes and the invisible language of HTML tags are not meant for human consumption. They are there for our computers, not for us. But when we rely on those computers to find interesting things and show us the results, we leave ourselves open to a new kind of vulnerability:

> If their points of weakness can be found, it is quite possible to trick our robots, like distracting a bloodhound with a scrap of meat or a squirt of anise–giving it the kind of thing it really wants to find, or the kind of thing that ruins its process of searching. The robot can be tricked, and the human reached: this is the essence of search engine spamming. (P. 113)

Brunton describes the current state of affairs, in which spammers and spam filters are locked in an arms race to master human linguistic patterns, as a parody of the Turing Test, "in which one set of algorithms is constantly trying to convince the other of their acceptable degree of salience–of being of interest and value to the humans." (P. 150) And in the book's conclusion, he circles back to spam's central irony:

> Indeed, from a certain perverse perspective … spam can be presented as the Internet's infrastructure used maximally and most efficiently, for a certain value of "use." … Spammers will fill every available channel to capacity, use every exploitable resource: all the squandered central processing unit cycles as a computer sits on a desk while its owner is at lunch, or toiling over some Word document, can now be put to use sending polymorphic spam messages–hundreds a minute, and each one unique. So many neglected blogs and wikis and other social spaces: automatic bot-posted spam comments, one after another, will fill the limits of their server space, like barnacles and zebra mussels growing on an abandoned ship until their weight sinks it. (P. 200)

Spam, in other words, is the cancer of the Internet. It is not an alien organism bent only invasion and destruction. Rather, it takes ordinary healthy communications and extrapolates them until they become grotesque, obscene, deadly parodies of themselves. Spam is constantly mutating, and it cannot be extirpated, not without killing the Internet, because the mechanisms they rely on to live are one and the same. The email is coming from inside the house.

Cite as: James Grimmelmann, *The Cancer of the Internet*, JOTWELL (November 12, 2013) (reviewing Finn Brunton, **Spam: A Shadow History of the Internet** (MIT Press, 2013)), https://cyber.jotwell.com/the-cancer-of-the-internet/.