Through a Prism darkly. What does software see?

Paper delivered at Conditions of Mediation
(conditionsofmediation.wordpress.com)
London 17 June 2013

Abstract

It is still a matter of debate whether the United States’ National Security Agency (NSA) had direct access to Facebook and Google’s servers. The NSA Powerpoint presentation suggests it did, the companies say it didn’t. What is clear however is that whatever the connection, it happened in and through software. Our digital detritus, the data, data trails and data relationships, was accessed, searched and organised through algorithms. Our standards-encoded detritus ensured our digital profiles could be standardised. Rather than looking at these issues through the human Subject, the spooks and what they can or can’t see, we can approach this surveillance and governmentality through unhuman objects and what they ‘see’ or connect with. This paper explores a particular software standard, JPEG, and its enfolding in Facebook’s governmental Open Graph. This algorithm can be seen as an object-actant in the manner of object-oriented ontology. Following Graham Harman this unhuman object can be seen as fully real yet weirdly withdrawn. Drawing on the work of Ian Bogost we can explore that object’s ‘experience’, perhaps even ‘perception’ of that world. By mapping the unhuman object-actants at work in complex computational systems, we can perhaps find a new way of approaching technological governmentality.

It is still a matter of debate whether the National Security Agency (NSA) had direct access to Facebook and Google’s servers. The NSA Powerpoint presentation suggests it did. One slide on the Prism presentation boasts of “collection directly from the servers of these US service providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple”. The companies say it didn’t. According to the
New York Times, there are perhaps secure online "rooms" where requested information could be sent and accessed by the NSA, but there is no ‘back door’.

Prism of course is not the only software surveillance and data-mining systems we know about. The Washington Post reported on a system wonderfully named BLARNEY complete with a cartoon insignia of a shamrock and a leprechaun hat, which describes itself as “an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks”. The equally evocatively titled Boundless Informant system, which analyses Prism data, reportedly uses free and open source software in order to make its data mining powers "available to all NSA developers" - a wonderful example of the rhetoric of open platforms coming back to haunt us, or at least watch us.

There is also debate over exactly what digital information the agencies were accessing: communications or metadata, the content of messages, postings and comments or information about those communications, time and spatial information, where and when the communication happened and between whom. What is clear is that whether sanctioned by the courts or not, whether direct or not, the NSA (and its UK equivalent GCHQ) have been ‘reading’ the digital detritus, the data, data trails and data relationships we leave behind online. This infinite archive of emails, messages and images as well as likes and shares are all objects that NSA’s software can build profiles and threat levels from. But in order for that surveillance, sorting and standardisation to work, the objects need to be not only accessible but readable and usable. If they are encrypted or in a non-standard format, the governmental machine slows down. The cryptographers have to get to work and the automated surveillance engine ceases to be as efficient.

Details of the specific software software Prism uses have still to come out. Palantir - named after a magical rock in Lord of The Rings that granted remote vision - a California Startup has denied that its Prism software is the one used. One could trace the myriad connections between the company, its backers, the CIA, Facebook,
Mark Zuckerberg, Sean Parker and its existing Government contracts to raise an eyebrow about that but what is perhaps more important is to note that data-mining, data-reading, data-sorting software is not only big business but at the heart of big business. Palantir says it sells "software that allows organizations to make sense of massive amounts of disparate data," and calls its software “financial analysis software”. Big Data and the software that see it, whether in a terrorist threat database, a loyalty card database or an RFID tracking database is at heart of the government of citizens and consumers. In Foucault’s terms it is governmental.

Prism, BLARNEY and Boundless Informant are examples of software “paying attention first and foremost to the intricacies of everyday experience” a dominant theme of media theory as we and no doubt GCHQ have read on the conference website. Those surveillance systems are also in tune with contemporary media theory in their rejection of ‘the audience” as an unmediated, general entity. Prism is about seeing differences as well as patterns, splitting the light of digital data as well as combining it. My aim in this paper is explore software as an object, to ask what it sees, to trace what it experiences. Working from Object Oriented Ontology’s starting point that everything can be treated as an object and Ian Bogost’s argument that “all things equally exist, yet they do not exist equally” I want to explore one software actant that we do know is in play between Facebook and the wider field of governmentality - JPEG.

In *Alien Phenomenology*, Ian Bogost asks what a camera sensor sees. Before we can unpack this puzzling idea, we need to go back to Object Oriented Ontology or Triple O’s starting point: that we can treat anything as an object and this enables us to remain rooted in the Real and escape what Quentin Meillasoux has called ‘correlationism’, the dominant philosophical tradition that simultaneously separates from and ties the human subject to a world of objects.

For Triple O, there are objects… Thinkers such as Bogost, Graham Harman, Timothy Morton and Levi Bryant are united in their commitment to widening the range of things we can see as objects, even imaginary ones like Harry Potter which while imaginary still have effects in the world; ones so large we can’t understand
them like climate change or weird ones like software standards. For OOO, objects are everywhere - real ones, material ones, human ones, unhuman ones, virtual ones… They are all, in some sense real because they all do things, have effects, connect with other objects. JPEG - the standard or codec - is weird. You can’t see it, touch it or, if you’re not a programmer, even find it in software outside of the Save-as option. But it is real. It does things. We can’t see it or touch it but its traces and connections are everywhere: in dot JPEG image files, in social media archives and search engine and hard drive caches, in data-mining strategies and surveillance practices, in business models. But like Keyser Söze, the mysterious figure in Bryan Singer’s film The Usual Suspects, JPEG just slips out of sight.

My aim here is not to discuss Triple O or the tensions within it around potentiality or materialism for instance but rather use it as starting point to explore software as an object, an object that connects with others in what Bryant calls a ‘democracy of objects’. To approach JPEG as an object-actant that ‘sees’ or connects is not a purely academic or philosophical exercise, it is a way of approaching Bogost’s question and the broader challenge of addressing the Prism-Facebook matrix.

Bogost discusses a digital camera sensor as an object and asks what it sees. This is perhaps an anthropomorphic gesture but not an anthropocentric one. His discussion of the Foveon sensor opens up questions of machinic perception and representation as well as the political-economic relations within which it is enfolded. This ‘metaphorism’, as he calls it puts the sensor in play as an object, worthy of analysis and critique. To map what it sees, how it works, what it connects with, the dimensions of its character that are available for those relations, is to open up imaging as a material assemblage of real conflict minerals and factories, sensual profiles encoding light as information as data as social data as surveillance data.

As I have noted, we cannot be sure what software the Prism system uses. But we can be sure that somewhere in that assemblage there will be JPEG - just so that the surveillance and data-mining algorithms can ‘see’ the image data encoded by my camera, your phone and Facebook’s servers. So, what does JPEG see?
JPEG exists inside - is that the right word? - software: a camera’s operating system. IOS7, Windows 8, Photoshop, Instagram, Google Chrome, Firefox, Prism and Facebook. Its sensual dimensions connect with a panoply of human and unhuman actants - photographers, face-recognition algorithms, databases, metadata mappers, photographers and spooks. The real JPEG - the Huffman and Discrete Cosine Transform qualities remain withdrawn but particular profiles connect as the photographer Saves as, the algorithm uploads and the panopticon sorts.

To anthropomorphise JPEG and ask what it sees is to open up those connections - the ones that Prism depends on and privacy advocates, terrorists and activists disrupt by using encryption and non-standard encoding. Let’s take as one example, the connection between Facebook and JPEG. Recall that if however Prism connects with Facebook data and metadata - whether directly or through a ‘room’ - its software connects with Facebook’s 240 billion JPEG-encoded photographs and therefore uses JPEG to decode those images to make them raw material for its own Prism graph alongside Facebook’s own Open Graph.

Let us look at digital imaging from JPEG’s point of view.

Take the example of a protestor, armed with their iPhone at a demonstration. When she presses the software button, light hits a sensor, an array of silicon, solar or photovoltaic cells. When light hits one of these cells, some of its energy is absorbed by the silicon, knocking electrons loose which are forced to flow in a particular direction creating a current: photons become electrons, light become electricity. At this point the light-as-electricity is still “analogue”. In order for the software (including JPEG) to be able to work with it, it needs to become digital. An analog-to-digital converter (ADC) then converts this electricity to digital information the RAW data file that is written to the camera’s storage medium.

JPEG then comes in. It ‘sees’ or connects with that RAW data in four ways. Firstly it samples, or connects with, the different frequencies, or colours in the data depending on how much they contribute to the visible image. Then JPEG applies a Discrete Cosine Transform (DCT) which readies the data for compression. Next
JPEG ‘rounds’ that data through ‘quantization’ and Huffman coding. JPEG’s ‘sees’ data, connects with it, sorts and compresses it. It adds details of the DCT and Huffman table to the final file that JPEG creates. JPEG has accessed RAW data and created visible JPEG data, ready for the imaging assemblage to use.

Our protestor then turns to her Facebook app and uploads the image. Because the data (including time and location information) has been encoded with JPEG, that data, image, record, proof is accessible by Facebook’s App software and the company’s upload server software. If she had taken a picture using a camera that encoded using the DNG standard or tried to upload a Photoshop encoded file, Facebook would not have been able to connect. Facebook’s software can access JPEG-encoded data. It can see it. The image is uploaded and the company’s Haystack system gets to work.

Haystack manages the huge amount of data and metadata Facebook generates. It is designed to spread the load and make searching, accessing and then using (tagging or liking etc) images as quick and easy as possible. When our protestor uploads her image it is reencoded through JPEG as four differently-sized images and added to her profile and her place in the Open Graph ready for her, her Friends, Facebook’s ad algorithm and Prism to connect with, sort, tag, file and share. JPEG - as a part of Facebook’s software - sees the incoming data and facilitates its fit into the Open Graph.

The JPEG-encoded data is now accessible from Web browsers - or data-mining browsers or software, as long as they too have the JPEG codec that can see and decode that file. Our protestor’s comrades around the world see her image because the JPEG standard built into the browser sees that Facebook image file, that data point in the Open Graph, can access the correct Huffman Table and DCT values to make that data visible. The human or unhuman agents in the NSA can see that image because their software has JPEG built in, seeing and reading the data and metadata readying it for other software to sort, recognise and arrange.
The democracy of objects that we have uncovered by following the object and what it sees is a governmental assemblage. Facebook’s JPEG-enabled Open Graph that maps and sets in motion what Carolin Gerlitz and Anne Helmond have called the Like economy and the NSA’s JPEG-enabled Prism Graph that maps and sets in motion what me might call the Threat economy are aspects of the managing of self and others that Foucault mapped as governmentality.

Following Charles Babbage’s idea of the difference engine we could perhaps call the Open Graph and the Prism Graph, relationship engines. As they track data relationships they generate new data. Each Like of an image or share is another data point to be mined and connected. Those relationships can be sold to advertisers or added to our NSA record as powerfully as the image itself.

It is not just that the JPEG-empowered Open Graph enable us to make and manage ‘Friends’, it enables us to manage our Self as Subject and as Object in social media space. Our JPEG-encoded and decoded avatar circulates, follows us, leads us and positions us under our choosing or not. When it appears next to a comment box or search results, when it is recommended to others, it oils the wheels of the Open Graph that Facebook builds its business on. Similarly, the JPEG-empowered Prism Graph manages our Threat identity along whatever database and software continuums are in play at any particular moment. JPEG-enabled metadata as well as visual data (itself open to face recognition software) circulates and connects as the JPEG standard object built into the next iteration of Boundless Informant sorts and standardises our images, imaginings and imaginings.

We could explore the potential of other objects - encryption or alternative codecs as ways of disturbing the Like and Threat economy that the Facebook-Prism is establishing. Of course NSA/GCHQ cryptographers would doubtless be more than capable of joining us in an encryption arms race, even if we do manage to slow the relationship engine down. Perhaps we could take Galloway and Thacker’s concept of the Exploit and look for the holes in that software hegemony that could be open to attack. Illegal DDoS attacks or legal swarms could swamp the systems - perhaps Facebook’s 1Bn partygoers are already doing that…
Whatever the tactics we use, what is important is to open up all the objects in play to analysis to ask, map and potentially challenge what they all do, what they all see.

The Author

Paul Caplan’s work explores software as an object. He uses practice-research - creating digital practice as a way of answering research questions - to explore issues of governmentality and visuality. A former photographer, journalist and digital consultant he recently received his PhD from Birkbeck, University of London and now teaches at Winchester School of Art, University of Southampton. His latest paper Software Tunnels Through the Rags ‘n Refuse: Object Oriented Software Studies and Platform Politics is forthcoming in Culture Machine and he is developing a book series that uses the affordances of mobile devices to create ‘Active Books’ that act as practice-research objects.