*Miriyam Aouragh*
Westminster University

*Seda Gürses*
New York University

*Jara Rocha*
Bau School of Design

*Femke Snelting*
Constant Association for Art and Media

# *Let's First Get Things Done! On Division of Labour and Techno-political Practices of Delegation in Times of Crisis*

## *Abstract*

During particular historical junctures, characterised by crisis, deepening exploitation and popular revolt, hegemonic hierarchies are simultaneously challenged and reinvented, and in the process of their reconfiguration in due course subtly reproduced. It is towards such 'sneaky moments' in which the ongoing divide between those engaged in struggles of social justice and those struggling for just technologies have been reshaped that we want to lend our attention. The paradoxical consequences of the divide between these communities in the context of the internet have been baffling: (radical) activists organise and sustain themselves using ‘free’ technical services provided by Fortune 500 companies. While alternative tech practices, like the Free Software Community, are designed, maintained, and actively used by a select few. We argue that even when there is a great desire to bridge this divide, the delegation of technological matters to the 'progressive techies' reconfirms hegemonic divisions of labour and can be as pertinent to this gap as political and philosophical differences are. Conversely, if our tools inform our practices and our practices inform our tools, then we will have to reconfigure these divisions of labour between 'activists' and 'techies'.

## *Introduction*

Our conversations on the topic started crystallizing at a workshop that took place at the 2014 Thinking Together Symposium, held at the Osthang Architecture Summer School, Darmstadt, Germany.[1It would only occur much later that our Darmstadt crew was brainstorming in a manner eerily similar to the constant dilemma within the politically motivated tech-activist scenes that we were trying to understand and challenge. We recognised that our pre-emptive questioning, pausing, and experimenting, and the necessary trade-off with going with the flow were mirroring that ongoing tension between thinking and doing. Our own occasional utterances of things like ‘Oh, lets first get things done!’ made us realise we were all projecting from our particular—professional, political, personal—contexts. We came to recognise how we mimicked the same logic of what we identified and critiqued as a normative western male-dominated approach that naturalizes hegemonic divisions of labor justified by a quest for efficiency
.
Our collective concerns are informed by narratives attached to: revolutions in the MENA region; uprisings in Gezi Park; the Indignados; the Free Software movement; and crypto-activist communities. We share a curiosity towards the pursuit of fundamental change that takes place at different political temporalities alongside techno-inventions. Time is never objective, and cannot be a standard empirical guideline, as our perceptions of time differ relative to personal struggles in a particular moment. The meanings ascribed to

time for instance depends on moments of stalemate, sudden moments of suffocating urgency, fresh moments of new possibilities, and commitments to re-making that may span a lifetime, or longer.  In any given moment, it is as if we are all placed within a matrix categorised by time and history; setting and locality; and technology, where each constellation brings another understanding of efficiency and urgency.

At historical junctures, like the ones we find ourselves in now, hegemonic hierarchies are simultaneously challenged and reinvented. Sometimes they are aggressively imposed, but often they are subtly reproduced; this is what we have come to refer to as 'sneaky moments.' These represent controversial mass-mediated events such as leaked secret-service programs. What matters is that in these sneaky contexts, hierarchies are also reconfigured by deliberate technological interjections. We propose that the divide between those engaged in politics of technology and those participating in struggles of social justice are being reshaped during those 'sneaky moments' and we argue that this reconfiguration requires reflection.

But, where do we start? What are ways to resist the consequences emanating from sneaky moments that impose a pragmatic submission to the specialisation of work or delegation to experts? How do we identify the well-meant efficiency that reproduces hegemonic divisions of gender, race, class and age, and that reinforces ideological differences between activists for social justice and activists for ‘just’ technologies (Dunbar-Hester, 2010)? And, how can we prevent tech-activists from becoming coopted by policy makers with geopolitical interests like the ones we have evidenced in Internet Freedom projects in the Middle East (Ben Gharbia 2010)?

We propose to begin identifying the problem through examples of mediation, investigating web-based campaign sites that claim to bridge the existing gap between social justice activists and progressive techies. Specifically, we look at sites that appeared or gained prominence at the onset of the public revelations about surveillance programs, as confirmed with the documents leaked by whistleblower Edward Snowden: our central sneaky moment. These campaign sites speak to the general public but especially encourage the use of secure communication tools for activists and journalists. But before we move onto this empirical analysis we first outline the critical reflections of activist use of media that has surfaced over the last years.

Our discussion explores responses to the Snowden revelations as relevant to the rise of campaign sites that promote secure communications. We further situate our analysis by introducing the actors we see as actively participating in the assemblage of activists and technology. [2] Our objects of analysis are the campaign sites that promote secure communications. Through these sites, we discuss how matters of delegation and division of labour are configured. Finally, we express our ideas concerning possible ways through which to rethink and possibly contest these hegemonic modes of operation.

### *Delegation to Platforms and Delegation to Tech-Activists*

The process of what we call delegation of technical matters to commercial platforms has attracted the attention of academics and practitioners alike. The growing critique of the use of these platforms for social justice movements has various components, and has become the focus of important critical debates in communication and media studies that are relevant to our analysis. Companies like Facebook, Twitter, or Google are designed to maximise the possibility to communicate more, which, when used in the context of progressive or radical change, leads to an integration of counter-hegemonic political movements into the grids of communicative capitalism. These platforms serve to capture attempts at resistance through the seamless integration of political projects into the communication-entertainment complex (Dean, 2009).

Nevertheless, in moments of crisis, as people leveraged these technologies to establish new alliances for radical change, the platforms run by these multinational corporations were elevated in mainstream media to the status of 'liberation technologies' (Mejias, 2012). This also meant that the companies running these commercial social platforms were presented as gatekeepers of 'internet freedom' [2].

The framing of corporate platforms as liberation technologies has overshadowed critiques of the profit agendas embedded in these monopsonies (Mejias, 2012). In the case of the Arab world, these kinds of projections have attributed to cyber-orientalism: the idea that ‘traditional’ people can be liberated by modern technologies, itself tied to a much longer history of essentialist representations of ‘the orient’ (Aouragh, 2015).

Other critics have argued that these platforms are sites for commodifying social labour, privatising social spaces, and subjecting dissenters to surveillance (Mejias, 2012, Fuchs 2009, Trottier 2014, Lyon 2008). The elementary functions delegated to these platforms—like the management of content—make activist groups susceptible to practices of censorship and algorithmic organisation of content guided by profit logics.

Profit on these platforms is a function of the number of users and their levels of interaction. Crucial to this dynamic is the curation of a conflict-free social zone. Given the entanglement between user interaction, profit and conflict, the blocking of users and content—that may cause tension—has become a central feature of these platforms.

Conflict management on social platforms, however, does not lend itself well to automation and requires expensive human labour. In order to contain the costs, conflict management disguised by the title 'content moderation' is outsourced to underpaid workers in Morocco or the Philippines (Chen, 2014). Paradoxically, delegating their technology matters to these platforms, counter-hegemonic activist groups become complicit with the labour conditions and logics of profit inherent to these commercial social platforms, that at the same time works to diminish their autonomy in organising their communications and actions.

In expectation and as a reaction to such developments, various communities have engaged in alternative socio-technical visions that integrate other forms of technological organisation.[3] Some of these activities have culminated in what has become known as the Free Software movement. As early as 2008 the Free Software community responded to the threat of increased surveillance and loss of privacy (Franklin, 2008). In their view, the use of centralised network services had grave consequences for how the internet, their most important working terrain, was developing away from 'Software Freedom' and freedom in general (Stallman, n.d.). Other groups, such as the Cypherpunks, focused on the development and dissemination of encryption based tools, which turned into a project of coding software that could 'make the networks safer for privacy,' and ensuring these technologies remain available to the public (Hughes, 1993).

While all of these groups are part of the story we are telling here, most important to our project is a small fraction of those progressive tech developers and advocates. Hereafter we shall focus only on those groups that have devoted themselves to putting in place infrastructures to protect activists from engaging in insecure communications. The activities of these groups gained momentum as news about internet surveillance and resulting government crack-downs became popular knowledge.

*Surveillance Revealed: A Sneaky Moment*

The urgency of the moment around the Snowden revelations saw tech activists respond with a design proposal to reinstate privacy: a call to 'cryptographic arms'. According to this techno-legal consensus the revelations make evident that the US government no longer limits its intelligence activities to military and diplomatic targets, but has exploited the 9/11 attacks on the World Trade Towers and the following War on Terror as a justification for engaging in mass surveillance across the globe. These efforts in surveillance have scaled so well thanks to advances in networked technologies and the dropping costs of processing and storage. So this is both an economically informed enterprise and one that is based on an artificial difference between mass and targeted surveillance. So within this consensus, mass surveillance is unacceptable as it reverts the presumption of innocence and violates people's privacy on the way to catching the 'bad guys', the subjects of targeted surveillance.[4] However, the shocking revelations regarding the NSA and GCHQ programs also undergirded the idea that if mass surveillance could be made inconvenient, somehow intelligence agencies would have to return to relying solely on methods of targeted surveillance. One way to make mass surveillance inconvenient is to make it costly. The idea is that if everybody, individuals and institutions, would use encryption, the cost of surveillance can be increased, stifling mass surveillance.

The immediacy of the problem as well as the apparent absence of any effective transnational laws that could be leveraged against these surveillance programs, combined with the call to stifle mass surveillance, culminated in different campaigns to encrypt 'everything' on the internet. While the main objective remained making mass surveillance expensive, encryption tools were paradoxically also seen as relevant for activists and journalists who were likely targets of intelligence gathering efforts.

These developments contributed to the momentum that saw numerous digital rights and internet freedom initiatives seizing the moment to propose new communication methods for activists (and everyday citizens) that are strengthened through encryption. This was paralleled by numerous conferences, blog posts, press articles, online and offline actions, and, central to our analysis, the development and promotion of encryption tools that 'enhance privacy'. This also coincided with a somewhat ironic acceleration in the flow of funds from US Department of State, Silicon Valley and philanthropic foundations to digital rights and informational self-defense projects.[5]

It is at this juncture that the necessity and desire for a convergence between those 'groups that wish to use the media instrumentally to draw attention to their political efforts versus those who wish to change the media system itself' (Carroll and Hackett, 2006: 86) became a matter of urgency. In response, a number of secure and private communication campaigns were launched or revamped, which also served to re-shape the delegation relationship between activists and this select group of technologists.

### *Conceptualising the Campaign Sites*

Some theoretical considerations are worthy of mention here. A clearer understanding of activism in the context of technology and therefore also a better (progressive, critical) assessment of technology in the context of political change requires some effort to conceptualise the terms and labels we often use. Earlier we referred to two camps that have been labelled tech justice and social justice activists. While the emphasis on the two camps may suggest they are mutually exclusive, the social implications of the internet for political mobilisation differ according to who they cater to: activists for or by technology and activists with or via technology (Aouragh, 2012). Certain people do their activism with political change as the objective and technology as the tool. For others, politics and justice is their context but a certain improvement in the tool itself is the objective. These overlapping identities and positions often shift or are part of parallel lives; in other words, some respondents in our respective research cases consciously divide between their techno-engagements for which they get paid and other political work that requires technology expertise they do for activist or ideological reasons. Changes in technology and technology governance, public space, labour conditions, and novel forms of organising also affect these divides and overlappings (Enrico De Angelis, 2015). Despite these nuances, our interest in this article is to draw out where these overlappings are negated, and to show how the divides are instated through socio-technical practices introduced in sneaky moments.

Another way of conceptualising our terms and labels is by deconstructing them, this is a similar but not identical exercise. For instance, with the Arab uprisings we learned that a proper assessment of the political implications of the internet depends on two different characteristics of technology: a tool for activists (operational, for example, coding or designing promotion material) and a space for activists (mobilisation, for example, expanding networks, archiving) (Aouragh, 2012).  The imminence of deconstructing terms and labelling fundamental to divisions of labor will become evident with our study of the campaign sites.

Furthermore, ‘tech activists’, far from a homogenous group, espouse a variety of political beliefs. These beliefs include attitudes towards design and how these matters translate to their activist practice. When it comes to gender, race, age, class and geography diversity among individual tech activists is less noticeable. This lack of diversity has been criticised from within and outside of the community. Certain civil society projects that produce campaigns can have a more diverse representation in gender, race, age, and geographical origin, for example, AccessNow or EFF. Still, those who are made prominent by virtue of a politics of representation that relies on viewership, tend to be white (Euro-American) and male, which is an important part of the re-instatement of hegemonic hierarchies between different activist groups.

Hegemony here is used in its vernacular meaning referring to dominance, but is also strongly linked to Antonio Gramsci's development and application. As Peter Thomas discusses—in what can be considered the most in-depth analysis of Gramsci—hegemony is a term that emanates from radical Marxist philosophy that has been disseminated via social scientists more than any other critical notion (Thomas, 2010: 133). Hegemony, in Gramsci's understanding, counters the false dichotomy between consent-based and coercive control. For Gramsci consent must be understood in its dialectical distinction to coercion. In constant interplay, they figure as 'moments within each other, theoretically distinct but really united as moments of a political hegemonic project' (167). So hegemony is complemented (but not necessarily) by coercion (for example, violence) and in liberal democracies often exposed through consent (for example, legal frameworks that are broadly accepted through media framings about its necessity), in the process contributing to the legitimization of the state. Hence, both our understanding of power and dominance, and of sneaky moments, fold into the critique of hegemony, and necessarily so in light of the role played by security initiatives during particular moments as discussed in this paper.

### *Rising to the Sneaky Moment of Surveillance*

Reflections on how the relationships between technology and social justice activists are being re-shaped is timely as we near the second anniversary of the Snowden revelations and the fourth anniversary of the MENA revolutions. In order to offer a critique, we studied several secure communication campaigns and analysed how they reveal their politics of mediation. While these campaigns exist alongside and in conjunction with training projects, we felt it was important to pay attention to the way these artefacts frame the relationship between tech activists and activists for social justice through language, selection, and design. From a large number of campaigns [6] that are currently actively being developed, we selected three sites and deliberately included a non-anglophone example:

- *Surveillance self-defense: Tips, Tools and How-tos for Safer Online Communications* [7]
- *The Guardian project: Mobile Apps and Code You Can Trust* [8]
- *Kem Gozlere Şiş: 'Bilgiyi şifrelemek, şifresini çözmekten daha kolaydır.' — Julian Assange* ('Encrypting information is easier than decrypting information.' — Julian Assange) [9]

Each of these projects proposes to address surveillance in a different way. The material ranges from full-fledged software 'solutions' to PDF pamphlets; from authoritative manuals to quick guides for people in a hurry. Often recycling similar arguments, references, methods, and software choices, awareness of surveillance is raised on these sites through an ever-expanding ecosystem of activities. While in some projects serious translation efforts are made, we were especially interested to see if the more situated initiatives would provide design elements that mediated between spaces of action with a different understanding of divisions of labor.

Before starting with a close reading and comparison of the way in which the content of the sites are communicated, we provide a description of the naturalised divisions of labour as enacted through the design, vocabulary, and other modes of address used in the campaign sites. Simultaneously, we look for conceptions of time and how the 'urgency of the moment' is being mediated through these sites. We later use this close reading for a broader understanding of the performance of these sites.

### *Devising Latent Structures*

The three campaign websites we survey are cultural artifacts, but they are also convivial spaces where various agencies co-habit with tools, discourses, and languages. In order to understand the dynamics of this complex scenography, we looked at the different gestures of delegation within these sites of mediation. By doing so, we started to identify some of the 'latent structures' that help us reflect on the situations in which these platforms function.

We argue that a dis-attention to the way the implicated agents (for example, the 'users', the 'developers', the tools, language and design elements) are mise-en-scène, results in a division of labour that follows 'traditional scripts', and shows a perhaps un-intended hierarchy based on traditional models of production. As a result, their performance can take a tragic and unintended shape in which tasks and articulations of labour tend to echo fixed behaviors. Such hegemonically-scripted actions imply a strict management of expectations from all implied agents. They are often the result of top-down hierarchies, naturalised to the extent of rendering divisions of labour invisible. This is why we refer to them as 'latent structures': while they are certainly present on these mediation sites, they merge with the background and move out of our frame of attention.

This merging with the background is a product of, but also facilitates, the path dependencies that determine both tool development and use, and as a result all the agents pass through it without interpreting it as a structure. In other words: its smoothness is a tricky materialisation of a long period of hierarchical organisation through a hegemonic performativity. This smoothness also has to do with a cultural paradigm of 'naturalizing the available' (Zapata, 2014). What this means is that agents perform within a pre-disposed framework, of which the limits, shapes, and shadows are no longer questioned, or may simply have found consensus: for example, in our case the assumption that a tool can provide security or enable anonymity. The reliance on available gestures is precisely the paradigm that helps merge latent structures to the background in our present (cultural, political) time.

When our cultural-political ecosystems intensify or enter moments of agitation, then our relation to tools tends to fall into the paradigm of affordances. It does not matter how radical the political struggle is, people may succumb easily to work with the available. Dependency on the available plot of technological design is precisely what produces the conditions for a sneaky moment, at the risk of discarding very basic political, ethical, and aesthetic sensibilities. To make these residues of our sneaky moment more tangible, we turn to exploring the secure communication campaign sites.

### *Designing the Divide Between Providers and Users*

The three campaign sites we have chosen are intended to mediate between the worlds of tech activists and social justice activists. We are interested in how they use language, design and tool-selection to bridge distances in knowledge, trust, and geography. If these projects are explicitly developed to communicate between agents that are not physically in the same space, how is a relationship of trust established? What do tech activists do to convince activists for social justice that they are on their side, and that the information and technologies provided are worth their trouble? And in the course of these relevant bridging and translation attempts, how do activists for social change find out if the provided tools are appropriate and safe for their situation? The three projects show similarities and also differences in their approach of how 'us' and 'you' are imagined.

A first thing to note is that both The Guardian project (TGP) and Security Self Defense (SSD) establish a clear separation of roles between those that provide these secure communication tools, and those that should consider using them:

> How to keep you and your communications safe wherever your campaigning takes you.[10]
>
> Whether you are an average citizen looking to affirm your rights or an activist, journalist or humanitarian organization [sic] looking to safeguard your work in this age of perilous global

> communication, we can help address the threats you face.[11]

This seemingly simple construction of address effectively sets up a narrative where tech activists in-the-know are reaching out to others, activists for social justice that might need their help. Interestingly, Kem Gözlere Şiş (KGS) is more ambiguous about their perspective, and will mix instances of 'us' and 'we/you':

> The objective of this project is to provide practical information about how to protect us from the 'evil eyes' that are watching us… As your knowledge of the issues and your skills increase, you will see that you can better protect your personal data and your privacy, you will feel more powerful.[12]

Given the precarity with which KGS was created, these shifts in mode of address could be due to a lack of professional copy-editing or the inherent elasticity of the Turkish language. However, their consistent ambiguity does suggest that the KGS tech activists might sometimes get out on the streets themselves. The site continues to invite readers to become part of a community: 'This project aims to help users who need privacy, to provide tips on how to protect oneself from 'the evil eyes' and to create a growing community engaged in these issues.'[13]

SSD imprints its signature on every page by mentioning that it is 'a project of the Electronic Frontier Foundation,', linking to the EFF project page. The connection with EFF attempts to provide authority and perspective to skip any mention of 'us' in the About page. Rather, the About page of the SSD campaign starts with explaining the type of users this guide is meant for, before moving on to the project's goals and limitations. In a secondary menu we find 'credits' and a list of individuals that have contributed to SSD. While credits are given for specific contributions, nothing is said about the institutional or political affiliations of these contributors. A similar lack of attention can be found at the KGS site. Some limitations of the recommended technologies are mentioned but there is vagueness about the identity of those who stand behind the site. TGP on the contrary has an extensive section 'About us' that explains 'How Guardian Helps', has all individual team members listed with 'anonymised' pictures and provides extensive details about funding and affiliations, including a note explaining that certain U.S. government related funding has not co-opted their work.[14] In all three sites, through omission or over-exposure of contributors, the stages are set for the rest of the information to come.

The campaign sites build on the assumption that many activists for social change are not familiar with the proposed methods and tools, that this threatens their activities, and that mediation is needed to change that situation. One important concern is hence usability: security and usability are typically seen as complimentary, if not competing aspects of secure communication tools. According to experts in the field, usability in this context means that 'it is easy for the users [using the tools] to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens anyway' (Sasse and Palmer, 2014)

Usability is addressed in two prominent ways. First, given that usability of security tools is tightly coupled with doing the 'right thing' and, in moments of urgency, the 'right thing' is ambiguous for activists, it seems like a reasonable choice that SSD and GP both employ 'scenarios' as the design method to communicate secure communication tools to their imagined or intended users. Through 'playlists' (SSD) or 'use-cases' (TGP) they categorise types of users according to their perceived security needs. In comparison, KGS does not provide explicit scenarios, but prefer to channel users' attention based on their devices: Mobile or Desktop. Scenarios in SSD are 'Activist or protester', 'Human rights defender', 'Journalism student', 'Journalist on the move', 'Mac user', 'Online security veteran', or someone who 'wants a security starter pack'. TGP on the other hand focuses on 'undercover human rights researchers', 'tech savvy citizen journalists' and 'activists in the streets', 'community organizations reporting on election issues', 'emerging online citizen journalists organizations', and 'mobile journalists for major news organizations.'[15]

Second, the three projects insist on communicating that the proposed technologies are easy-to-use. SSD literally offers a 'security starter pack' that is a manual which starts with threat modelling. TGP makes an effort with seven friendly icons ('So you got an Android phone?') each linking to an up-beat interactive explanation, consistently starting with 'Easy'. Both sites use design styles and language that mimic commercial on-line services. KGS evokes the 'security pack' with big red buttons suggesting one-click-install.

In usability design, a scenario is a description of a person's interaction with a system. It is believed that scenarios help focus design efforts on the user's requirements (Nielsen, 1993). The scenarios here though seem to directly map existing technological solutions onto supposed real-life experiences; they are predominantly organised around assumed groups of solutions or technologies rather than in response to actual problems. An indication might be that most of the images and icons used on the three sites depict devices, rather than situations. Another issue that none of the scenarios brings up is situations that might ask for solutions not based on technological tools. The mantra of 'simplicity' hides the complicated and situated nature of using the promoted technologies in real-life situations, and designs away the human efforts that need to be made to put the advertised technologies into action.

From the awkward connections between technology needs and skills, causes and effects, devices and situations we started to wonder who was involved in the establishment of those categories. If these tech activists have already established relationships with activist groups on the street or in human rights initiatives to think through the required technologies and to test and develop them together, then the effort to communicate via a website is in fact redundant. On the other hand, if the projects are set up to actively reach out to unknown activists for social change, supporting a dialogue between groups is essential. SSD has a 'feedback' button on each page, but omits any possibility to ask for a return on the feedback. A secondary menu offers a standard contact form that is protected, but does not allow for any further secure forms of communication—for example, through email. The 'help us' that is repeated on most pages at KSG, includes the following rather conversational statement: 'We ask you to inform us about mistakes in any of the documents we provide. If you have suggestions for better solutions, please let us know. You can also contact us with questions about use.' Users are invited to send comments and suggestions by Twitter, indy.im, and Diaspora. When we first tried out the site, their email address had become invalid, which probably explains why the FAQ—which has great potential for communication—has remained empty. TGP states on their contact page 'If you’d like to learn more about Guardian from the team directly or have a proposal for us, please let us know using of the methods below'. The Guardian-Dev Discussion List is potentially the most interesting channel for user-provider exchange, as it invites developers as well as power users or 'just anyone interested in getting involved in the development side of things.' But even if this list may be read as the most inclusive of all three campaign sites, the listing of profiles centres again on technological development and negates any space for a collective exchange beyond this specific area.

By speaking to the activist audience rather than inviting them into a community of participation, the campaign sites in fact unnecessarily amplify the condition where activist communities are not expected to take part in the definition of the relationship they will have with the technologies they apparently need to depend on. Participation in activities that shape these secure communication tools is hard, but will be even less appealing (or even not known to the users) if not explicitly solicited. If problems appear, users will abandon tools that do not match their context. In moments of urgency, the drop rate may depend even more so on the urgency and needs of the activists rather than the positivist claims made on these sites.

### *Connecting Technologies to Situations*

The activists may need to develop their own scripts of the possible ways in which tools can fill in roles during different moments of activism. Currently, sites like Security Self-Defense by EFF, as is also typical in many cryptoparties, starts by asking users to do 'threat modelling'. As phrased on the website, 'To become more secure, you must determine what you need to protect, and whom you need to protect it from.' While threat modelling is a tool in itself that can be useful for activists, its military and industrial origins are ever-present.

In professional settings—such as within a company or the military—threat modelling is assumed to be part of a number of activities conducted by a large team of developers: for example, when there is a bigger system development or maintenance project where security is one aspect among many. The language of 'assets' assumes that the owner of the system has (information) assets that need to be protected, and it is the security team's duty to make sure those assets are secured. This monolithic vision of a system to be defended is however outdated and criticised within security engineering. Even a corporate system is likely to have users and associates with conflicting interests, meaning that there may be numerous competing threat models, for different situations, the priority of which depends on the bigger project that is to be achieved as well as the priorities of different actors (Pfitzmann, 2001). Addressing the social and political complexity of threat models would allow the SSD site to show that security is a negotiated process, instead of a clear state of affairs which experts can discover depending on their adversaries' capabilities.

Further, all the examples in SSD focus on information assets and relevant data, which may or may not be of primary importance for activists. Hence, the campaign site sees threat modelling through the perspective of the tools they offer: the tools are there to secure information, hence the activists should focus on securing information. This is very different than focusing on people, situations or political goals that may matter to the activists, which may or may not translate to 'information assets' afterwards.

Instead, all three projects claim, at least on the surface, to aim at the same type of users, under pressure of similar threats. It is in this context surprising how little overlap there is between suggested technologies. While both SSD and TGP are involved in developing software themselves, the first layer of each of the campaigns seems to focus on the curation of useful technologies, bringing them together in easily digestible 'playlists'. In these playlists, besides ChatSecure and Tor plus related software for phones, Orbot and Orweb, there is not always consensus between projects. This partially reflects the SSD's implicit tendency to focus on desktops and laptops, and TGP's explicit focus on mobile technologies, but the reasons for focusing on different hardware remain inaccessible to the audience of the campaign sites.

What is also surprising, given that these sites are about security awareness, is that only SSD provides timestamps for the information that is presented. Campaigns may have starting dates, or the websites may contain reference to the year when the site was last updated; however, they lack prominent timestamps that would be useful to indicate whether the information is fresh or outdated. Given that security vulnerabilities are disclosed every day, this leaves the users with the duty of checking whether these tools are still valid for use. The 'weatherrepo' federated app store is an initiative of the Guardian Project that hopes to provide an app store with vetted tools. While this is a timely project that could address the problem of continuous vetting, it is ironic that the weatherrepo information page states information about Yahoo! mail that is no longer valid.[16]

### *A Wider Lens on Divisions of Labour*

The issues we highlighted so far point to an underlying division of labour through the distribution of roles according to expertise, in other words based on specialisation of work. The latter is most typically evident in the distinction drawn between developers and users. This division inevitably comes with expectations towards and assumptions about the capacities of each role. Foremost, it frames a dependency relationship and situates the expertise inevitably with the developer. In other words, the developer is seen to have the necessary and probably sufficient skills to develop a given technology (Suchman, 1994). Especially in matters such as security, where threats and vulnerabilities to the underlying protocols require extensive technical skills, this seems like a plausible delegation. But, is it?

For activists across parts of the Arab world, the conditions of their activism are increasingly being shaped by encroaching danger and enclosure. Rather than a widening of activist networks, maintaining their physical, social and political momentum has become priority. In this context, what an activist expects when organising or mobilising via the internet (and mostly social media) is that it works. In working with these communities, our cautions about long-term risks involved with relying on commercial social networking platforms and our encouragement to engage in co-designing alternative infrastructures is at times met with bored sighs, pitying smiles, or confused stares. During a political tipping point, such as an uprising or the eve of a massive public occupation, users want efficient and ready-to-hand tools. Activists may not have the time or the patience to become designers too.

These statements are a residue of what popular commercial services are expected to offer—an expectation that normalises the delegation of numerous matters to developers and commercial platforms. Such unquestioned delegation confirms the latent structures that cement the power asymmetries between users and service providers. However, even in using these services, there is always some friction that is not captured by the developers, and here the activists hope that another division of labour within the movement will solve these: tech savvy activists can volunteer their time to making sure there is connectivity and that the tools work while others storm the streets. During tipping points, time is so valuable that it is not very wise to raise any question about pragmatic delegation decisions based on specialisation of work.

In the context of commercial platforms, this may come at the price of blocked accounts, adhering to real name policies, the frustration of having to manually recreate a friends list of a blocked account, or waiting for language features to be implemented: for example, Arabic hash-tags in Twitter.[17] These consequences affirm the motto that activists are opening their practices to change according to the tools that they use.

An engagement with alternative tech activists sensitive to their needs has the potential to reverse some of these dependencies, however, the campaign sites that we studied suggest that this is not guaranteed. While many of the secure communication tools are revolutionary in their protocol design, the campaign sites indicate that the same tools rely on very traditional framings of users and ways of relating to developers and technology. Expectations of a seamless service combined with inattentiveness to how their relationship is framed folds activist users and progressive developers into the available forms of delegation. This sets up the 'users' to oscillate between deliverance to developer decisions and disappointments with unsatisfiable expectations. In the pursuit of making complex encryption tools accessible to users in a format that they would recognize from commercial platforms, we find that the campaigns sites in fact amplify the user-developer opposition.

*Design from Nowhere in Service of Activists*

Focusing on usability pushes the task of integrating these tools into everyday practices onto the activist communities. It takes great amount of labour to integrate any new tool into the social tapestry that activists find themselves in. With every tool comes the laborious activity of configuring them to local needs, maintenance of tools on the variety of available devices, as well as the development of trust toward the tool developers through mechanisms like 'user support.' Given that these laborious activities are critical to secure communications, it is a concern that almost none of the campaign sites attend to these matters, and generally do not consider how people can move into the secure communication space collectively. In the pursuit of usable tools, the collective labour necessary to use them goes unrecognised.

In that sense, these campaign sites that aspire to bridge between tech developers and activist users succumb to a commodification logic. The objective of these sites is to depict security tools as 'completed products.' Due to the lack of salience given to timestamping, the continued validity of the security and availability of the tools, as well as to the developer-centric modes of production comes to resemble a project of 'design from nowhere' (Suchman, 1994). According to Suchman, this is an ideal in which:

> the goal is to construe technical systems as commodities that can be stabilised and cut loose from the sites of their production long enough to be exported en masse to the sites of their use (Suchman, 1994)

Subjecting secure communication tools to a commodification logic demands that security is a binary—you can download and be secure—a somewhat unachievable goal. This expectation pressures developers of secure communication tools to either come up with gross security claims or disclaimers that some of these tools may not work, pushing them to further confirm the illusion of a universe in which security exists as a binary.

This is a significant step away from the culture of secure communications. Practitioners participating in what can be called security design collectives will agree that 'it takes a village to keep a tool secure' and that security is a continuous 'cat and mouse game.' But this culture is lost on the campaign sites. With the exception of the empty FAQ on the Kem Gozlere Şiş site and the developers channel on The Guardian Project, there is little invitation on any of these sites that gesture at the idea of creating an activist community that can collaborate with the developers. This mode of mediation sets up the individual user 'to be the weakest link' instead of playing for the 'community to be the strongest link' in achieving a security aware activist culture.

### *Universalising Tools for Global Users*

The objective of developing tools that can function across contexts is part of the universalist ideal typical of design collectives. Here, in the absence of far away users under threat, designers can invoke them at will and imagine their needs (Oudshorn et al., 2004). With the urgency to build secure communication tools that are easy to install and use independent of context, this practice becomes further normalised. Justified by a similar sense of urgency, some tech activists promote getting funding for a tool through, for example, Internet Freedom initiatives focused on `dissidents in repressive regimes', which can then also be used by activists in so-called democratic countries. These pragmatic and politically troubling steps lead to many contradictions. For example, it makes it possible for campaign sites to reach out to users across the world, while the devices that are required to install the proposed tools assume users have access to some of the latest in mobile technologies and infrastructure.

Security design collectives also have the additional objective to make sure that the security guarantees of the tools that they develop are 'exogenous, homogeneous, predictable, and stable, performing as intended and designed across time and place' (Orlikowski, 2007). These tools are however entangled in very intricate political and social realities which technologists can only 'design around' to a limited degree. Nevertheless, in security engineering practice, the ambition to develop tools with universal security properties is seen as an ideal and is pertinent to modes of thinking that allow engineers to abstract away from situated knowledge of a specific context and to shift real world problems into the technical solution space. This means that developers can pursue goals like developing an anonymous communications service like Tor, which provides anonymity or the ability to circumvent censorship regardless of contextual constraints.

Yet, while the design of anonymous communication networks is a challenge in itself and validates the need to abstract messy realities away, user community input can be almost as pertinent. In fact, the Tor community has been very aware that Tor can only work if they take situated reporting into account. When the act of using Tor, which can be identified by ISPs, can be sufficient to put a person under suspicion, it becomes evident that contextual realities matter and the design of tools has to be rethought.[18] Other times, local conflicts cannot be designed away and activists already under suspicion may simply be better off staying away from these technologies. This situation was expressed most articulately by Anne Roth, when her family was put under heavy surveillance in Berlin, Germany for unsubstantiated terrorism charges. Similar conditions hold for many members of the 'Muslim community' in the US and Western European countries, who do not necessarily have the luxury of securing their communications, as this would trigger greater suspicion and surveillance. Technology design requires focusing on the security of activist interactions on the network, but other variables may creep up in unexpected ways. This requires tech activists to continuously revise their social, political as well as technical assumptions. As a consequence, it is very challenging, if not undesirable, to rely solely on technical experts to develop technologies for activists.

The heavy reliance on tech activists also conceals an effective international division of labour which all of the campaign sites affirm. What Mike Hales put into words in 1994 about corporate engineers still proves to be true in the context of progressive tech developers:

> Our times present us with a de facto economic and cultural separation between production and use. In our work world, producers are professionally (i.e., culturally) specialized; to a large extent,

> system-production is located in specialized and distinct sectors and/or geographical locations within an international division of labor (Hales, 1994)

In addition to the tendency for tech activists to develop universal technologies with a 'design from nowhere,' much of the development work occurs in the Western hemisphere where market values of efficiency and resulting coding practices are the rule. As more and more tech activists succumb to the pressure to develop ready-to-hand tools, this also means they are expected to replicate designs whose success is based on market parameters. This is the point at which most of the campaign sites and tool developers evaluate their success on the number of downloads or number of individual users rather than the efficacy of the tools for the projected activist communities. Once subject to these parameters of market efficiency and its correlated principles of design, questioning of hegemonic divisions of labour can only be regarded as counter-productive and inefficient.

A related anxiety among activists is that technologies tend to shape their environment towards increasing individualism (one of the features of social networking) and that this hinders collective action. A telling example is given at the Fourth Arab Bloggers Meeting in Amman (January 2014). This challenge was voiced during a heated debate about ways to bridge the gap between knowledge and practices of activism, more precisely how blogging can shift from an individual act to a more comprehensive collective performance. The internet motivates micro-celebrities and social media stars, and this tendency is further triggered by traditional media where some bloggers and activists are put in the spotlight, treated as if they were spokespersons for the entire movement (Angelis and Della Ratta, 2014).

In an interesting reflection during the conference by a Yemeni activist, we are reminded that the dominant or expected hierarchies of priorities cannot be universalised. The person in question mentioned that in the surge of social media trainings, they often don’t take into account the needs of local societies, especially in terms of anti-surveillance programs:

> Circumvention is not a big issue here; yet we heavily invest in training on such tools in every single event, conference, and gathering held in this region. Rather than the currently very hyped issues of cyber security/anti-surveillance, finding a safe offline space to meet and plan is of a much greater concern (quoted in: Angelis and Della Ratta, 2014)

### *Let’s First Get Things Done: Modes of Operation for Sneaky Moments*

One way to better situate some of the secure communication development activities is to move from an attitude of 'design collectives' at the service of (individual) users, to 'designing for activist collectives'. This could be bootstrapped by avoiding inscribing users into the language of threat modelling, and instead inviting security engineers to step into the language of collective action within a political project.

For example, our experiences from the Arab world, Turkey and Spain suggest that the stage (or timing) of certain actions defines how relevant a tool is and what potential it may entail for a given action. A helpful way to think through these contradictions is to imagine a distinction between various stages of a revolution: pre-revolution (preparation and mobilisation); moment of revolution (the actual tipping points); and post-revolution (successful continuation or dangerous counter-revolution). It is useful then to juxtapose these historical timing-related factors with the kind of usage (sometimes as a space and at other times as a tool).

This distinction in time suggests that technology is not always the dominant driver of change but surely is one of the actors of change. This insight is relevant for understanding which tools, infrastructure and group —the activists for technology/activists with technology—are best suited or should be more present at a given moment. Depending on these different phases, it may be more informative to rethink how the use of secure communication tools may be decisive (for early mass mobilisation), just mentionable (for class struggle) or virtually irrelevant (in military battles [17]).

Further, by framing the matter at hand in terms of the role of technology for activists in the context of the aforementioned Pre/During/Post categorisation of the political moment, it may be valuable to start by distinguishing what effect we expect technology to generate for political activists or politically motivated techies. Technologies may tip the scales of power when they help expand existing networks and thus become vital for the emergence of movements and campaigns. This can be achieved by interpreting the online/offline divide as a reflection of the space and tool separation, and this in turn as part of the overall political strategies and tactics without excluding any of the pre- or non-digital technological tools or spaces.

Reframing the project of communications security as a constituent part of political activism may however still reproduce the user-developer dichotomy. A more radical proposal may be to shift this relationship by recognising that ultimately what is desirable is to do 'collective design'. Here, the way in which Lorea, an alternative social network, proposed to frame the relationship between activists and technology provides some inspiration:

> These networks are self-managed because Lorea is a non-profit, independent, open, and self-sufficient project. We don't talk of 'users' but rather of 'inhabitants' because we prefer a conscious coexistence instead of a simple, passive client relationship. Lorea inhabitants actively participate in the design, development, and maintenance of the network's working to implement the federation protocols, develop code, maintain safe servers, hunt down bugs, translate the interfaces into various languages, test user friendliness, document its development, and to undertake dissemination, help, or welcome activities for new inhabitants. There is thus no institution or formalized association behind Lorea, but rather a community of inhabitants.' (N1Crew/SpiderAlex)

What is beautiful about the proposition of 'inhabitants' here is that it explicitly recognises the labour it takes to make a 'community tool'. Where Lorea probably had its shortcomings was in their inability to sustain the project and the costs of labour over time. For many tech activists, although not all, the dependency on wage-labour is something that they can free themselves from, at least temporarily (Soderberg, 2014). This ability to sustain oneself is, however, both gendered, raced and geographically constrained, if not also specific to the IT sector.

A focus on divisions of labour that defines roles based on their relationship to the software artefact leaves out the fact that the production, maintenance and use of the technology can only exist with the necessary sustenance of life, such as the production of food and shelter, for the reproduction of labour power. In many political collectives with their own space, this is also known as the problem of 'who pays the rent' and 'who cleans the toilets.' In fact, a lack of attention to matters of sustenance of life has been the breaking point of many alternative projects, if not the point in which corporate and government funding has found entry into alternative technology projects.

In talking about costs, it is important to circle back to the argument by tech activists that proposed an economic solution to end the NSA and GCHQ surveillance programs by raising the cost of monitoring through the use of encryption. We may sadly find that in this sneaky moment, the tech activists forgot to add to their equation the cost of integrating secure communication tools into the practice of social justice activists. In fact, the urgency of our post-sneaky moment maybe to think along the lines of class, regional differences, as well as too easily assumed divisions of labour, if we want secure activist communication projects that truly scale.

As revelations about surveillance programs and related crackdowns on activists have emerged, tech activists grasped, remoulded, and redefined this occasion. They effectively translated what are considered surveillance problems into one concerned with privacy and cryptographic self-defense. We attempted to develop a vocabulary and offer a snapshot that could help us attend to the naturalised divisions of labour and technology delegation practices that manifest themselves between activists for social justice and activists for just technologies during such sneaky moments. In order to situate our discussion, we focused on the numerous initiatives that emerged to provide activists with secure communication tools, seizing the momentum created by the anxiety about surveillance. Retrospectively, this turn happened almost naturally and invisibly, sneakily extending fringe secure communication tools to activist communities across the globe. The subtext in such initiatives invokes the notion of a universal user and in extension that of a universal activist. This is where it started to sound familiar; the hegemonic division of labour related to universalist ideas about technology came to conceal situated politics, interests, and contestations.

These projects make a lot of sense in a world where governments and its services cannot be trusted. The proposed alternatives promise to protect activists from uninvited eavesdroppers and resulting vulnerabilities, while continuing to use internet-based services. In doing so, the campaign sites channel the vacuum created by the revelations about surveillance programs into building trust around encryption technologies. They vet small tech activist initiatives for secure communications and vouch for their trustworthiness so that they can scale globally. Due to their sudden prominence, these sites also serve as hubs for delivering public trust towards internet-based services. To rephrase: the sudden rise of these campaigns is not coincidental and for a variety of reasons have also found support from Fortune 500 internet companies and governments scrambling to rebuild confidence in the internet and associated markets (Wisniowski, 2012).

In summary, we illustrated how these campaign sites transform tools developed by tech activists by delivering consensus around using the available structures for reframing secure communications technologies: for example, by depicting them as usable apps that are one-click away. In contrast to the careful articulation of politics through a diversity of tools, we found little attention given to the delegation relationship that is constructed between the invoked activists and the tech developers.

The user-developer opposition reiterated on these sites gives insights into how specialisation of work and scarcity of resources can easily lead to divisions of labour, expressed across fault-lines of race, gender, class, age, and geography that are themselves already a consequence of neoliberal power. As a result, tech activist communities and social justice activist communities, ideally a natural match, come to oppose each other in these 'sneaky moments.' Our critique comes with its own risks. Given the positive valence associated with these campaigns and the largely marginal position of counter-surveillance initiatives, our critique may be seen as overburdening these small projects. Yet, we argue, given the impact and potential of these initiatives, critique remains necessary.

*Biographical Note*

Miriyam Aouragh is an anthropologist and Leverhulme fellow at the Communication & Media Research Institute of Westminster University, UK.

Seda Gürses is a computer scientist working as a Post-Doctoral Research Fellow at the Media, Culture and Communications Department at NYU, USA.

Jara Rocha is a cultural mediator and a core member of GReDiTS/Objetologías research group at Bau School of Design in Barcelona, Spain.

Femke Snelting is an artist and designer, member of the association for arts and media Constant in Brussels, Belgium.

*Endnotes*

[1] Thinking Together Symposium—August 2014 http://www.osthang-project.org/projekte/thinking-together/?lang=en

[2] Internet Freedom, U.S. Department of State http://www.state.gov/e/eb/cip/netfreedom/index.htm

[3] As the 'social' has become increasingly 'networked', several free software projects have tried to address

(some of) the critiques of the way in which dominant companies began to shape social networks. These contestations on sites like RiseUp https://help.riseup.net, Mayfirst https://mayfirst.org, or Lorea http://p2pfoundation.net/Lorea are manifested through modes of software production and design proposals that are expected to enable novel performances of notions like politics, transparency, privacy, security, freedom, the networked social, and infrastructure autonomy.

We are not impartial towards these projects or their ambitions. The Darmstadt Delegation came together on the basis of a shared experience of troubling differences in the politics, values and practices of 'activists for social justice' heavily using networked technology for their struggles, and of 'tech-activists' who struggle to develop progressive and alternative technologies. In conversation with numerous initiatives that have aligned around Backbone409 (Calafou, http://backbone409.calafou.org), interference (Amsterdam, https://interference.io/), transhackfeminist! (Calafou http://transhackfeminist.noblogs.org/), noisy square (OHM https://noisysquare.com), and the internet ungovernance forum (Istanbul https://iuf.alternatifbilisim.org/), we are concerned that due to pragmatic decisions in times of urgency and lack of resources, these struggles may subscribe to divisions of labour that reproduce existing hierarchies and dominant discourses and practices.

[4] In this argument, targeted surveillance is bounced between either being legitimate, and hence not worthy of further discussion, or out of the scope, since technical solutions cannot withstand methods used by a keen nation state adversary targeting an individual, community, or country. Both assumptions are problematic. First, intelligence agencies do not make the distinction. Second, the artificial distinction forecloses initiatives that address how decisions are made to target people, communities, and countries and what targeting entails. Third, it reduces the argument to an economic one, i.e., it is about increasing the costs of surveillance, depoliticizing the topic matter
.

[5] A sample of some of the funding reports that has been flowing into digital security projects: DRL Internet Freedom Annual Program Statement for Internet Freedom Technology, http://www.state.gov/j/drl/p/207061.htm; Portfolio Assessment of Department of State Internet Freedom Program: An Annotated Briefing, http://cryptome.org/2014/09/rand-internet-freedom-attack.pdf; Digital Defenders, https://digitaldefenders.org; Knight News Challenge on Strengthening the Internet, http://www.knightfoundation.org/blogs/knightblog/2014/6/23/19-projects-win-knight-news-challenge-strengthening-internet/

[6] An overview of campaign sites that we considered can be found here: Media:Theatreofsurveillance.jpg

[7] Surveillance Self-Defense (SSD) is a project by the Electronic Frontier Foundation. The aim of Surveillance Self-Defense is to teach people how to think about online privacy and security so that they can adapt their choice of tools and practices in an ever-changing environment. The project is framed as a defence against the abilities of modern technologies to eavesdrop on innocent people. Some of the proposed tools are developed by the EFF themselves. EFF is based in the United States and funded by individual donors, NGOs and some corporate support. https://ssd.eff.org

[8] The Guardian Project (TGP) is developed by an international collective of software developers embedded in the Free Software community. They observe that mobile technologies are important for communication and collaboration, but problematic when it comes to personal security, anonymity and privacy. In response, the Guardians actively develop software applications, software libraries, customized mobile devices and tutorials. The project is funded through donations from NGOs around Human Rights issues such as Free Press Unlimited and Tibet Action Institute, as well as the US Government's funding schemes for human rights projects that are channelled through the Department of State and Radio Free Asia. The Guardian Project also receives support from software related companies such as Google, and from philanthropic foundations. https://guardianproject.info/

[9] Kem Gozlere Şiş (skewers to evil eyes) is a project developed by members of Alternatif Bilişim (The Alternative Informatics Association) in Istanbul, Turkey. Resisting the 'evil eye' of surveillance, the project addresses users in Turkey to prevent them from bringing their security and privacy in danger through careless use of communication devices. Kem Gozlere Şiş offers a software selection and related manuals in varying degrees of detail. Kem Gozlere Şiş is a volunteer project organised by members and the activities of Alternatif Bilişim receive event based funding from various local and international NGOs. https://kemgozleresis.org.tr/tr/

[10] Security Self-defense, Landing page. https://ssd.eff.org/ Last Checked: November 2014.

[11] The Guardian Project, Landing page https://guardianproject.info/home/partners/ Last Checked: November, 2014.

[12] Kem Gözlere Şiş, Landing page https://kemgozleresis.org.tr/tr/kemgozler/
Last Checked: November, 2014.

[13] Bilgiyi Şifrelemek, şifresini çözmekten daha kolaydır. Kem Gözlere Şiş, About this project https://kemgozleresis.org.tr/tr/kemgozler/

[14] Note: this project has received small grants and sub-contract work from organisations (such as the Open Technology Fund) and research projects (such as Tor) that receive funding from the U.S. Government and other governments around the world. None of this funding has modified or shaped our development plans, and we would never, ever put any sort of backdoor or compromised component into our software based on this funding. https://guardianproject.info/home/partners/

[15] How Guardian helps https://guardianproject.info/home/use-cases/

[16] WeatherRepo https://guardianproject.info/code/weatherrepo/ The webpage claims that Yahoo! transfers mails in the clear, a statement that no longer holds since the company defaulted to a secure protocol for webmail in 2014
.

[17] Here we are assuming the situation in which the infrastructure is totally destroyed, as is the case in the recent battlefields in Syria. In the same country, geolocating individuals, food sources, neighborhoods if of interest to the Syrian regime, as well as US and EU funded NGOs. When information about the location of bakeries and food queues turn out be important for attacks by the regime and intelligence gathering by foreign governments, information security can indeed be very relevant. (See for a sample of such surveillance http://caerusassociates.com/wp-content/uploads/2014/02/Caerus_AleppoMappingProject_FinalReport_02-18-14.pdf )

[17] Twitter is now available in Arabic, Farsi, Hebrew and Urdu https://blog.twitter.com/2012/twitter-now-available-in-arabic-farsi-hebrew-and-urdu

[18] See project on Tor Pluggable Transports, developed in response to increased use of DPI by Internet Service Providers to detect Tor users https://www.torproject.org/docs/pluggable-transports.html.en

*References*

Aouragh, Miriyam. 'Social Media, Mediation and the Arab Revolutions', *Triple C Journal* 10.2 (2012), http://www.triple-c.at/index.php/tripleC/article/view/416

Aouragh, Miriyam. 'Revolutions, the Internet and Orientalist Reminiscence', in Reem Abu Fadel (Ed.) *Visions of Tahrir: Connection domestic and international spheres in revolutionary Egypt* (London: Routledge, 2015).

Carroll, William and Hackett, Robert. 'Democratic Media Activism through the lens of Social Movement', *Theory, Media, Culture and Society* 28.1 (2006): 83 - 10
4
Chen, Adrian. 'The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed', *Wired*, 23, October (2014), http://www.wired.com/2014/10/content-moderation/

Dean, Jodi. *Democracy and Other Neoliberal Fantasies: Communicative Capitalism and Left Politics* (Durham, NC: Duke University Press Books, 2009).

De Angelis, Enrico and Ratta, Donatella Della, 'Mind the Gap: Bridging Knowledge and Practices of Activism' at the Fourth Arab Bloggers Meeting, Jadaliyya, June 7 (2014), http://www.jadaliyya.com/pages/index/18040/mind-the-gap_bridging-knowledge-and-practices-of-a

De Angelis, Enrico, 'Introduction: The hybrid system of Egypt and “cultural chaos”', *Égypte/Monde arabe*, March 25 (2015), http://ema.revues.org/3398

Dunbar-Hester, Christina. 'Beyond 'Dudecore'? Challenging Gendered and 'Raced' Technologies through Media Activism', *Journal of Broadcasting & Electronic Media* 54 (2010): 121—135.

Franklin Street Statement on Freedom and Network Services (2008) http://autonomo.us/2008/07/14/franklin-street-statement/

Haggerty, Kevin D. and Richard Ericson. 'The surveillant assemblage', *British Journal of Sociology* 51.4 (2000): 605—622.

Hales, Mike. 'Where are designers? Styles of Design Practice, Objects of Design and Views of Users in CSCW', in D. Rosenberg et al. (eds) *Design Issues in CSCW*, Springer (1994): 151—177.

Hughes, Eric. ‘A Cypherpunk's Manifesto’, 9 March (1993), http://www.activism.net/cypherpunk/manifesto.html

Mejias, Ulises A. 'Liberation Technology and the Arab Spring: From Utopia to Atopia and Beyond', *Fibreculture Journal* 20 (2012) http://twenty.fibreculturejournal.org/2012/06/20/fcj-147-liberation-technology-and-the-arab-spring-from-utopia-to-atopia-and-beyond/

N1crew/SpiderAlex. ‘Reclaim the Networks: Technological Sovereignty for Social Networks’, https://n-1.cc/blog/view/76157/reclaim-the-networks-technological-sovereignty-for-social-networks

Nielsen, Jakob. *Usability engineering.* (London: Academic Publishers, 1993): 99

Orlikowski, Wanda J. 'Sociomaterial Practices: Exploring Technology at Work', *Organization Studies* 28 (2007): 1435—1448

Oudshoorn, Nelly, Rommes, Els, and Stienstra, Marcelle. ‘Configuring the user as everybody: Gender and design cultures in information and communication technologies’, *Journal of Science, Technology and Human Values* 29.1 (2004): 30—63

Andreas Pfitzmann, Multilateral Security: Enabling Technologies and Their Evaluation, *Informatics Lecture Notes in Computer Science Volume 2000*, (2001): 50-62

Sasse, M. Angela and Palmer, Charles C. 'Protecting You', *IEEE Computer and Reliability Societies*, January/February (2014): 11—13

Soderberg, Johan. 'Reproducing Wealth Without Money, One 3D Printer at a Time: The Cunning of Instrumental Reason', in Stefan Meretz (Ed), Book of Peer Production, *Journal of Peer Production* (2014), http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/reproducing-wealth-without-money/

Stallman, Richard, 'Who does that server really serve', https://www.gnu.org/philosophy/who-does-that-server-really-serve.html

Suchman, Lucy. 'Working Relations of Technology Production and Use', *Computer Supported Cooperative Work (CSCW)* 2: 21- 39 (1994): 21—39.

Thomas, Peter. *Gramscian Moment: Philosophy, Hegemony and Marxism*, (Chicago, IL: Haymarket Books, 2010)

Wisniowski, Matthew. *Engineers for Change: Competing Visions of Technology in 1960s America*, (Cambridge, Mass: MIT Press, 2012).

Zapata, Guillermo, 'Ni el copyright ni el copyleft te va a dar de comer', *El Diario*, November 13, (2014) http://www.eldiario.es/interferencias/copyright-copyleft-va-dar-comer_6_324127601.html