CENTER FOR ADVANCED INTERNET STUDIES

Thomas N. Cooke

Oscillation, Feedback, and Time: iOS as a Cybernetic Control System

CAIS Report

Fellowship
April bis August 2018

GEFÖRDERT DURCH

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen

Oscillation, Feedback, and Time: iOS as a Cybernetic Control System

Or, How Jailbreaking (re)Establishes Time as a Crucial Dimension of User-First Privacy

Introduction

What is the sociopolitical significance of digital conflict between Apple and jailbreaking hacktivists who re-engineer iPhones for alternative purposes? Why are these hacktivists interested in re-engineering corporate technology, in what ways, and for what purposes? Since the initial release of iPhones in 2007, hacktivists began breaking into them almost immediately. A central motivation surrounded Apple's choice to increasingly "close off" their operating systems in the name of user security and privacy. However, numerous hacktivists contended that such efforts signalled the emergence of a double entendre. While closing off an operating system with novel encryption techniques positioned Apple to claim they are protecting user data, it also positioned Apple to dominate the mobile application marketplace (Freeman, 2008). Moreover, the closing-off of the operating system also allowed Apple to discriminate which applications users can install. One category of applications unapproved by Apple's closed operating system and marketplace design are privacy-enhancing applications, precisely because the manner in which they operate not only exposes the closed operating system design. They also open the system up to external design critique, which compromises Apple's highly regulated application marketplace business model, and the data flows that propagate it.

At the heart of the digital conflict between Apple and jailbreaking hacktivists is thus the matter of why a closed-source design has persisted for so many years, particularly as the premise upon which this design has been defended is politically motivated (Zetter, 2007; Arthur, 2012; Brewster, 2015). There are considerable social and political stakes in this conflict. One of primary interest is the role this conflict plays in framing how users themselves socialize into and understand the notion of 'digital privacy'. While Apple's closed-system design indeed protects some user data, it tends to privilege *content* data. For example, the words of an email or text message. What it tends *not* to cover is *metadata* – the math, so to speak, of content data itself. This latter kind of data is increasingly problematic for user digital privacy and is not the kind of data that Apple's closed systems are designed to protect. As the project argues, this is because the unfettered flow of metadata – between approved marketplace applications and software developers' third-party advertisers – is central to Apple's business model. 'Digital privacy', according to Apple's closed-system imagination, is at direct odds with a jailbreaking hacktivist perspective that seeks to protect *all* data – not just content data. The project contends that by opening up Apple operating systems, so as to allow the installation of otherwise banned privacy-first software, such as ProtectMyPrivacy (PMP), users will learn about digital privacy in a more critical, comprehensive, and heuristically motivated way.

Cybernetics as Important Groundwork

In order to understand precisely how Apple's closed-system design socializes users into expecting a particularly narrow representation of digital privacy, the project demonstrates that iPhone users are guided to implicitly associate 'content data' with 'digital privacy'. The project's argument is demonstrated by revisiting the twentieth-century technoscientific theory of cybernetics, which is rendered into a critical epistemology intended to assist us as analysts in understanding how an iPhone's operating system (iOS) trains a specific kind of user experience.

Cybernetics emerged after the Second World War as a scientific theory of how *communications systems* – both machinic and organic – can be understood as *control systems* (Wiener, 1948). Initially celebrated throughout the academy as an innovative interdisciplinary endeavour involving a team of engineers, physicists, and mathematicians, the theory emerged not only due to the intersection of numerous mutually beneficial philosophical interests, it also emerged out of a mutually beneficial desire to address practical problems. Applied cybernetic theory made a notable influence on the refinement of military systems throughout the Cold War. In doing so, it also became highly influential upon the computational sciences – influences which are both explicitly and implicitly measurable today (Halpern, 2014).

One of the largest appeals of cybernetic theory is the conceptual robustness of many of its core tenets: 'input/output', (negative versus positive) 'feedback', 'homeostasis', 'oscillation', and so on. What cybernetics thus provides academic problem-solvers is a teleological toolkit; to examine systemic issues, behaviours, and solutions, in terms of goals. Accordingly, systems are defined in terms of 'input' data, provided internally or externally, which is processed as valuable information required to guide the system towards its goal. As the data is processed, the system evaluates how and whether that data is useful. The basis of that evaluation is determined through the process of 'feedback', where some of the 'output' information a system produces (as it pursues its goal) is judged in terms of its effect on system performance. If the system's feedback validates that its goal-seeking path is reliable, accurate, and useful, it is deemed 'negative' feedback. 'Positive' feedback, on the other hand, is deemed inaccurate and as such, detrimental as it steers the system off course. Too much positive feedback produces what is called 'oscillation' – the regular displacement of a system in an unproductive fashion.

The project re-deploys cybernetics here not as a way of solving Apple iPhone problems. Rather, it is used to critically understand their behaviour, achieved through a technoscientific epistemology – a way of intellectualizing how iPhones see, know, and manage data and its users. Accordingly, the project argues that iPhone operating systems (iOS) are also *governance systems*, ones which steer technical and social behaviour. As Pangaro (2013) deftly iterates, cybernetic systems are not merely technical but also social because the essence of cybernetics is political. Cybernetics originally emerges in Platonic philosophy as a governance strategy – it is not just a twentieth-century theory. Examining themes of continuity in iOS's visual, aesthetic design, this project explores how iOS trains users to imagine data and privacy in specific ways.

Analysis and Critique: iOS from a Cybernetic Perspective

While iOS has indeed been critiqued as a closed system from a security and privacy coding perspective, they have also been criticized for being inflexible at the level of user customization. Users have not enjoyed the same freedom of design experienced by, for example, Android users. But what this strictness affords Apple from device to device, era to era, is an ease at which applications, settings, and information can be found and acted upon by their users.

For example, consider how the booting process, icon layout and size, and screen-swiping processes have virtually remained the same across eleven years-worth of iOS designs. While the argument can be made that Apple is simply providing familiarity for users, this continuity can also be critically recognized

as an attempt to control how users expect and experience data, security, and privacy. Consider how Apple has seemingly invested in adding depth to 'settings'.

Since iOS 6, Apple has designed more and more sub-menus within the settings component of iOS (Frakes, 2012), manifesting in the form of visual 'sliders'. These sliders provide an 'on' or 'off' capacity, essentializing the user as the gatekeeper over how and whether applications can receive data from the device's sensors, libraries, emails, and so on. But as the project argues, these sliders are overtly binary in nature. They either allow access, or prevent it, in absolutes. If access is denied, the application cannot function, which disincentivizes and effectively invalidates the user's decision-making altogether. Apple is not merely engineering a sense of control here. They are also engineering epistemic spaces, which has direct effects on how users think, see, and behave when using their iPhones.

From a cybernetic perspective, consider how the submenus and sliders represent dimensions of a control system that create for the user a perception about data. The perception of particular interest here is that 'all data is the same'. The user is a cog in a machinic system whose goal it is to maximize data flow in the name of entertainment and profit. If the user perceives an application to be hostile to the user herself, it thereby must also be hostile to the order of the system in which she is intimately embedded. By turning off access of an application to, for example, emails and text messages, she protects herself and the system. However, and because this experience is defined within the absolutist nature of binary privacy and security sliders, the question of precisely what data – from where, in what size, what form, and with which significance – is un-addressable. The user is effectively compelled to manage all data through a judgement capacity without context to threat and risk. The only notions of threat and risk are articulated externally – from news headlines, for example. But the system itself cannot be the source of the problem. Threat and risk are imagined by the user as external issues, but never from within. By co-opting the user into a control system that does not preview nor discuss contexts of threat, risk, and data insecurity, the system ensures the creation and flow of negative feedback.

iOS thus directly mediates how users think about data and privacy. The security sliders are nothing more than indicators of how data flows should be regulated. The technical data-management processes taking place, however, cannot be seen, studied, or questioned; the user is providing a specific kind of input on the surface level of a closed system that cannot be opened up. Even if she wanted to learn about the processes, in the name of trust for example, it is virtually impossible to do so. How data is protected remains secretive, and thereby compels blind trust in processes she cannot access. More significantly, the majority of the data being handled is content data – not metadata. As Apple cultivates the spaces within which users make decisions, they are also cultivating spaces in which security and privacy are rationalized. In the case of iOS, and since its release in 2009, we as analysts must recognize that users have been encouraged to think about and handle data in ways that are conducive to Apple's marketplace business model – one which depends upon user ignorance about metadata.

This is not a novel revelation amongst hacktivists. In fact, it is precisely the inability for users, auditors, developers, IT security experts, and academics to see, study, understand, and control discrete metadata flows (those which play a role in how smartphone users are profiled as consumers and security threats) that compels jailbreaking in the first place. Understood as the technical process of breaking into the root-level of iOS so as to liberate user customization and facilitate the installation of otherwise disallowed software, jailbreaking is indeed a direct modality of digital protest and activism (Chen, 2009; Hestres, 2013).

Of particular interest to the project is "ProtectMyPrivacy" (PMP). This jailbreaking-enabled software empowers the user over how iOS creates and circulates metadata to applications, specifically by interrupting the metadata transfer process itself. The user is warned about these flows and provided multiple options to decide how and whether that data continues to flow. This process also involves a crowdsourcing element, which puts the user in touch with other users so that they may collectively construct the meaning and significance upon which a more critical understanding of privacy and security unfolds.

These kinds of software interventions are actively resisted by Apple. After close analysis of the timeline of iOS updates, this project demonstrates that an average of 12 micro-updates are released between every major iteration of iOS each year. In doing so, Apple disables any jailbroken devices and related software from functioning. This process is critically explored in the terms of cybernetic oscillation, whereby the input of jailbroken software, along with its introduction of what may otherwise be deemed as alien coding, destabilizes Apple's control over precisely how metadata flows inside an iPhone. This also destabilizes Apple's ability to mediate how users understand data and privacy. PMP displaying metadata to users is a direct intervention in the design and spaces within which users socialize into and experience security and privacy. In effect, jailbreaking displaces Apple's ability to persistently cultivate and control user input as a modality of negative feedback precisely because PMP interrupts this process by educating users about the nature of the otherwise unfettered flow of metadata within and outside of the iPhone.

In conclusion, this project argues that through digital-level conflict over how users experience data, (and, in turn) security, and privacy, we as analysts can think about digital privacy from the 'bottom-up' as opposed to the 'top-down'. There is indeed a significant difference between corporately-oriented and controlled digital privacy versus digital privacy premised upon data visibility and legibility as provided by hacktivist communities. Findings on this project have been published in the surveillance studies field-leading, peer-reviewed journal of *Surveillance & Society* (Cooke, 2020).

Bibliography

Arthur, Charles (2012). Walled gardens look rosy for Facebook, Apple – and would-be censors. *The Guardian News,* 17 April 2012 [28.10.2018].

Brewster, Thomas (2015). Apple Builds Another Walled Garden – Around iPhone Ad Blockers. *Forbes Magazine,* 20 October 2015 [27.10.2018].

Chen, Brian X. (2009). 6 Reasons to Jailbreak your iPhone. *Wired Magazine,* 8 July 2009 [28.10.2018].

Cooke, Thomas N. (2020). Metadata, Jailbreaking, and the Cybernetic Governmentality of iOS: Or, the Need to Distinguish Digital Privacy from digital privacy. *Surveillance & Society* 18 (1), 90–103.

Frakes, Dan (2012). *Hands on with iOS 6: Safari*. Retrieved from https://www.macworld.com/article/1168499/hands-on-with-ios-6-safari.html [21.10.2018].

Freeman, Jay (2008). *Bypassing iPhone Code Signatures*. Retrieved from http://www.saurik.com/id/8 [29.10.2018]

Halpern, Orit (2014). Cybernetic Rationality. *Distinktion: Journal of Social Theory,* 2, 223–238.

Hestres, Luis E. (2013). App Neutrality: Apple's App Store and Freedom of Expression Online. *International Journal of Communication,* 7, 1265–1280.

Pangaro, Paul (2016). Why Do We Want To Live In Cybernetics? *Cybernetics and Human Knowing* 23 (2), 9–21.

Wiener, Norbert (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine.* Massachusetts: MIT Press.

Zetter, Kim (2007). iPhone's Security Rivals Windows 95 (No, That's Not Good). *Wired Magazine*, 23 October 2007 [29.10.2018].

Table of Figures

Photo Titlepage: CAIS, Matthias Begenat

Contact

Dr. Thomas N. Cooke
The Surveillance Studies Centre
Queen's University, Kingston, Canada