CRYPTOME BETA REPORT
to
NYC Department of Information Technology & Telecommunications
Regarding LinkNYC Beta

Cryptome infiltrated the beta-testing phase of LinkNYC during Spring 2016 – pro bono publico – for the public good. Pro bono publico underscores Cryptome's mandate as New York City-based architects licensed by New York State to address issues of public health, public safety and public welfare (HSW). Field photographs documenting our survey of LinkNYC kiosks in their technological and urban context are provided as an exhibit to this beta-phase proposal for HSW-conforming design remediation for LinkNYC, hereby submitted to NYC DoITT.

https://cryptome.org/2016/06/linknyc-spy-kiosks-installation-videos.htm

Deborah Natsios and John Young, Cryptome, NYC July 24, 2016

INTRODUCTION

Sidewalks enjoy pride of place as New York City's regnant public domain. Their infrastructure of gritty pavement underpins democratic mobility, hosting tens of thousands of named and nameless pedestrians who glide at their own pace along 12,750 miles of the city's concrete pathways on foot, stroller and wheelchair. Dress in stylish costume or down-market denim. Hum, sing, speak aloud to yourself, to companions or into a smartphone. Test the ergonomics of sidewalk furniture at a bus shelter, parking meter, mailbox, wood bench or newspaper dispenser. Urban personhood is embodied on this pedestrianized stage during self-directed performances of sociality, anonymity, window-shopping and commerce.

The sidewalk's man-made rhythms strike intensely personal counterpoints against the thrum and roar of vehicular transit. Uptempo negotiations conducted with traffic signals jazz up the citywide matrix of 12,460 intersections. Despite the ambient throng and frenetic pace -- poet, caregiver and office worker command a sense of agency over their inviolable private and social selves during these street-side processionals. The shock of any disruptive confrontation on the pavement only confirms expectations of rights to an integrated pedestrian self.

Where the regulation of sidewalk infrastructure is required, that task falls to the venerable NYC Department of Transportation (DoT), which monitors the installation of reinforced concrete pavement, steel-faced drop curbs, crosswalks, traffic signals, handicap accessible curb cuts and the special requirements of

historic districts. DoT will also inspect sidewalks for improper slopes, trip hazards, wayward tree roots and collapse.

COMMONS

What new regulation of the sidewalk's rich tableau of public experience is being promoted by self-described 'smart' cities, which harness information and communication technologies (ICT) to manage municipal processes? Smart goals introduce ICT and new efficiencies to free market doctrines that, in recent generations, invoked the putative 'tragedy of the commons' to devalue public space.[1] That colonizing trope rejected the public commons as a failed collective of depleted resources. Only privatization could capture and fully monetize the value of an urban resource.

A private conservancy now manages Central Park. The corporate atrium, a privately-owned public space provided in exchange for developer air rights, is enforced by prohibitions and private policing. One unintended consequence of such deals finds a billionaire presidential candidate luxuriating in a triplex penthouse granted by air rights exchange -- just as the presumably public atrium at the base of his elite tower is suddenly subject to law enforcement's increasingly coercive restrictions.

What will the impending economic privatization of the sidewalk's shared realm mean for our equitably democratic access to New York City? Monetization of the dynamic pageant of urban democracy embodied on the sidewalk stage may exploit and corrupt pedestrian privacy, autonomy and agency. This question has been provoked in Spring 2016 by the inaugural installation of LinkNYC technology, a next-generation overlay onto the existing thicket of vintage sidewalk systems. Compliant stenographers of the press have largely ignored the product's concealed interests when announcing its rollout of a network of free public Wi-Fi hotspots as a replacement of the city's obsolete pay phones, of which 7,302 grime-encrusted examples remained in 2014.

Installed onto the block-by-block legacy footprint of the public pay telephone network, the private LinkNYC matrix will eventually total some 7500 (possibly up to 10,000) touchscreen sidewalk kiosks across the city's five boroughs in what is described as the “largest public municipal Wi-Fi system in the world.”[2] Ads displayed on 55” HD screens will reportedly fully subsidize a public ICT benefit offering free public Wi-Fi hotspots with a coverage of 150 feet, 1G high-speed internet access, USB charging ports, free domestic phone calls and assorted emergency call buttons.

Questions about the extensive network remain unanswered. What undisclosed hardware and software are bundled in this initial public release or may be retrofitted in future upgrades? Are the kiosk's smart city technologies market-driven innovations whose primary goal is to optimize the global city brand for

shareholder profit – at the expense of public space's democratic equity? Will purported benefits indeed mitigate or, instead, exacerbate the public crisis of income inequality, social stratification and exclusion that are among obdurate signatures of the 21st century global city?

Users committed to a democratic city are entitled to robust transparency about the workings of any municipal system's disclosed and undisclosed frameworks. Such municipal transparency has been obscured by a kiosk design which conceals cameras, microphones, sensors and reporting hardware and software that will be transmitting real-time big data to centralized command-and-control entities. In order to serve the public benefit and prevent civic harm, Cryptome beta-tests suggest the kiosk should undergo hazard-resistant redesign modifications that disclose and articulate currently camouflaged platforms and outcomes.

New York City hopes LinkNYC can help bridge the digital divide that has withheld broadband access from 27% of city households.[3] Yet in recent decades, municipal governance has been less interested in digital equity and information equality than in harnessing ICT and Big Data to regulate metropolitan processes. A municipal scale Internet of Things (IoT) is wiring legacy infrastructures into hybrid assemblages shaped by market-driven, risk management best practices. These privatizing regimes anticipate and control urban outcomes through risk calculations that will mine data and metadata from myriad sources, as David Lyon has described.[4] Flows of data and metadata culled from ubiquitous devices are the raw resources that fuel big data analytics for anticipatory urban governance and risk management doctrines of preemption that can stratify, profile and divide. Risk management doctrines of preemption profile and pre-criminalize – by definition. Not everyone benefits equally from the highly targeted regulations of a risk-averse, aggressively profiling city.

GROUND TRUTH

Next-generation technologies for anticipatory governance mount special challenges against the sidewalk's vibrantly adhoc democracy. Such a challenge is being mounted by an eponymous pop-up corporation, Sidewalk Labs Inc., which co-opted the name of the pedestrian's legacy domain to underscore its claim of innovative solutions to 'big urban problems.' A Google spinoff, Sidewalk Inc. holds the controlling interest in the LinkNYC consortium granted a 12-year franchise by New York City in 2014. Entities cycling through consortium membership are variously named as Qualcomm, Intersection (a merger of Titan and Control Group), Comark, Civiq, CityBridge and Google's parent company Alphabet Inc. Sidewalk is the lead investor in Intersection, self-described as the country's largest municipal media company, which will run the kiosk system and its ad-generated revenue stream.

Sidewalk Labs Inc. has lubricated the lucrative revolving door between public

service and the profit-driven private sector in its staffing practices. CEO Daniel L. Doctoroff was deputy mayor of economic development and post 9/11 rebuilding in the pro-business Bloomberg administration from 2001-2008, and President and later CEO of the business and financial news giant Bloomberg LP from 2008-2014.

Doctoroff promises to advance the Google spin-off's market prospects through ongoing opportunistic relationships: “Sidewalk will affiliate itself with more companies as time goes on, whether through acquisitions or investments.”[5] He announces that “Sidewalk ultimately plans to make money in different ways” revealing a potentially problematic vision of subscription models for real-time data platforms harvesting ground truth from streets and sidewalks of “completely connected streets.”

LinkNYC success in New York City's challenging milieux will be a marketing bonus for the business development unit planning the product's global expansion. Cities in the US and around the world who have abstained from installing similar systems are assessing the prototype as can only be beta-tested in an elite global city.[6]

Sidewalk's goal of exploiting completely connected streets reflect its parent company's boundless appetite for ground truth data. Doppelganger technologies concealed beneath the culturally visible surfaces of LinkNYC's tower design recall covert Google practices that triggered lawsuits and investigations in 38 US states and 12 foreign countries.[7] Google Street View vehicles plying the world's roads with concealed Wi-Fi receivers had captured personal data transmitted over unencrypted public Wi-Fi networks, without user consent. Google admitted “unintentional” culling occurred in more that 30 countries between 2008 and 2010, capturing payload data that included emails, usernames, passwords, images, and documents.

Google's attempt to refute plaintiff arguments that the culling was a breach of the US Wiretap Legislation Act underscores the regulatory distinction between unregulated Wi-Fi and cellular and radio signals regulated by the FCC. Vulnerabilities of LinkNYC public Wi-Fi may be exploited without federal intervention, making Wi-Fi a preferred conduit for deregulated data transmittal. The vulnerabilities of Wif-Fi's deregulated bandwidth suggests it may be no accident that no LinkNYC kiosk has been installed on the block where Google headquarters is located at 111 Eighth Avenue – where one might otherwise be expected.

BATTLESPACE

Google's dominant interest in harvesting ground truth is written in the subtext of LinkNYC marketed to potential advertisers as a context-aware platform for placement of ads 'relevant' to users and neighborhoods. Relevant ads targeting

web browsers may infiltrate user behaviors and preferences in the virtual spaces of laptops, tablets and smartphones. But covert, context-aware technology targeting the geolocated social and political spaces of embodied urban neighborhoods for relevant ads are another matter altogether. Such context-aware technologies automate and database a more troubling kind of socioeconomic and geographic profiling of the already segmented city, as David Lyon outlines.

Context-awareness technology of the kind that will enable LinkNYC's privatization and monetization of the urban sidewalk without pedestrian awareness or consent also plays a powerful role in the military imagination. Omniscient dreams of 'situational awareness' undergird the ethos of conquest in the digitized terrain of next-generation battlespace. The army recruiting motto “be all that you can be” applies to warfighters as well as dual-use technologies that serve the full spectrum of both military and civilian interests.

What does LinkNYC's context-awareness technology for manufacturing ground truth along completely connected streets mean in a key global city whose counter-terrorism efforts since 9/11 have included the automation of situational awareness to identify ambient threats relating to asymmetrical warfare. Downtown Manhattan's Domain Awareness System of 6000 surveillance cameras developed with the help of Microsoft is a case in point. Its sensors report upstream to the war room of the NYPD Joint Operations Command Center (JOCC), the high-tech command-and-control nexus installed next to Police Headquarters after 9/11. As a complex technical system, LinkNYC is similarly managed by a sophisticated command-and-control regime that may be readily appropriated by political expediency.

Recent precedent demonstrates that when necessary, the state of emergency will intercede in the rule of global city and its vital infrastructural hubs. Business as usual and civil liberties are summarily suspended and all urban assets requisitioned during such states of exception. The civilian platform of a dual-use technological dyad will be toggled to the military pole. Urban anonymity that is a cultural privilege and civil liberty of the democratic street and sidewalk is anathema to situational awareness operations. Captured in visage, voice, movement and scent – the anonymous pedestrian cannot be ruled out as a potential sidewalk combatant.

Argonne National Laboratory is partnering with the LinkNYC consortium to develop real-time 'intelligent attentive' sensor arrays for use in the citywide matrix.[8] It has been claimed, but not publicly displayed, that 30 such sensors are present in the LinkNYC kiosk. Cryptome requests to the consortium for information about the sensor arrays have not been answered. Evidently, context awareness is a one-way diagram when it comes to information sharing.

LinkNYC's working relationship with Argonne reveals the national interest in the convergence and crossover of military to civilian applications of advanced technology like wireless military sensor networks – WMSN – engineered for extreme context sensing and context interpretation. Weaponizing a civilian context-awareness devices is consistent with Stephen Graham's description of the new military urbanism in which military goals of high-tech omniscience are applied to the governance of urban civil society.[9] Fusion of policing, military and intelligence techniques and technologies is doctrinal, but also seeks the commercial expansion of dual-use products into lucrative civilian markets. Graham points to the “massive boom in a convergent industrial complex encompassing security, surveillance, military technology, prisons, corrections, and electronic entertainment.”

The Pentagon has funded, equipped and, many observers note, incited local police with war-grade military gear. Militarist culture and performance are transferred along with hardware. Military grade C3i was once the industry standard for analysis, optimization, intelligence-gathering, feedback, and synthesis. Now C4isr (command, control, communications, computers, intelligence, surveillance and reconnaissance) provides operational frameworks for what Graham describes as “the extension of military ideas of tracking, identification and targeting into the quotidian spaces and circulations of every day life.”

The manufacturer of the LinkNYC kiosk, Comark, is a specialist in mission-critical automation. Comark vaunts its weaponized, ruggedized line of military computers, displays and secure operating systems that offer “USB port disable option, prevents unauthorized USB devices.” Investments in the fusion of policing, military, intelligence techniques and technologies means ubiquitous infrastructures like LinkNYC's ground-truth harvesting sensors will not remain unproductively fallow. States of emergency call for ground truth to be culled whenever para-military crisis management supersedes normal civil procedures. Such practices inexorably filter into the more quotidian civic realm.

JURIDICAL

With the block-by-block matrix of powerful context-aware sensors poised to operate as a massive antenna harvesting ground truth across New York City without pedestrian knowledge or consent, LinkNYC has installed a governance regime that operates just across the legal boundary of predatory captures of urban Big Data. Only the slim paperwork of boilerplate privacy policy replete with the negative language of denial stands between hardware and software already in place, or easily retrofitted, that can toggle-on weaponized situational awareness with the flick of a switch. In a prime example of tongue-in-cheek denial, LinkNYC management assures the press and public that “Link cameras are currently inactive and are not designed to feed into any NYPD systems.”[10]

Yet LinkNYC privacy policy remains compliant, stating that enabling the system's covert platform will be left to the discretion of the court's juridical framework. Massive datasets that capture the anonymized sights and sounds of lovers' quarrels, Black Lives Matter protesters, students reading James Baldwin aloud or *solfeggio* spilling out of brownstone windows may be de-anonymized and geolocated.

Can a privacy policy ever truly supersede the latent operational potential of a design? LinkNYC users should challenge fine-print claims that kiosk sensors will not collect data from or about consumers. That facial recognition technology will not be used. That video footage of the surrounding area captured by kiosk cameras will not be kept for longer than seven days “unless the footage is necessary to investigate an incident.” That video will not be shared with the city or governmental law enforcement “unless legally required to.” That “we will not use our cameras to track your movement through the city.”[11]

PRO BONO PUBLICO

Cryptome infiltrated the beta-testing phase of LinkNYC during Spring 2016 – *pro bono publico* – for the public good. *Pro bono publico* underscores Cryptome's mandate as New York City-based architects licensed by New York State to address issues of public health, public safety and public welfare (HSW) as lynchpins of professional practice.

Cryptome's beta-testing fieldwork for HSW conformance includes photographic documentation of the network and a review of key benchmarks expressed by New York City in its initial solicitation of 2014 “Request for Proposals for a Public Communications Structures Franchise.”[12] These provide the basis for proposed design remediation of the kiosk to mitigate public hazard and encourage a transparent public infrastructure.

Cryptome's beta-testing challenges mainstream reporting on the Franchisee rollout, expertly stage-managed by the consortium's sophisticated PR retinue. Media reports ranged from uncritical tech boosterism about fast connectivity to cautionary warnings of possible civil liberties threats, as were raised by NYCLU in a March 2016 letter to the Mayor.

LinkNYC declares 90% of public thinks the network is a positive development. Cryptome's beta-testing hopes to expand user awareness. This exercise in public education aligns with the Public Service Announcements LinkNYC states it will occasionally provide on the kiosk's 55” HD screens.

New York City cites public benefit as a key driver of its 2014 solicitation: *“It is the City's intention to maximize the public benefits under this franchise and to ensure that all New York City communities benefit from the services and the local economic opportunities presented by this initiative.*” We examine below the city's

claim that civic infrastructure for a public ICT will promote social equity in the global city's knowledge economy.

Cryptome visited hundreds of Link kiosks during field surveys of Spring 2016. Photographic documentation captures urban impacts of the installation process, from trenching, pulling fiber, laying re-bar, pouring concrete to lowering kiosk cabinets onto their pedestal by truck-mounted hoist – a phase of work executed without proper protections to unwary public walking beneath. This public hazard must be corrected promptly.

Cryptome photographs of the street-side installation process are a reverse-engineering exercise that exposes a rare public overview of the cabinet's proprietary innards. This exposée of black-boxed elements provides clues for how to make the system more transparent in democratic frameworks.

Finally, photographs document structures as they have begun to be used in the social context of the city's diverse neighborhoods, including historically under-served communities. Preliminary observations reveal that as a practical matter, New York City's hope that the kiosks will help bridge the digital divide for households without broadband is belied by the structure's inhospitable design, which seems to intentionally limit use to short term episodes. The free-standing towers offer no privacy, no sheltering protection from the elements and no perch for sitting as provided by the legacy public pay telephone cabin. Anything other than brief uses are effectively discouraged.

Anecdotal interviews with users in under-served neighborhoods reveal their concerns of vulnerability while exposing mobile devices to potential phone-snatchers, not least in the dark after hours of a 24/7 network. Users in under-served communities heavily targeted by police surveillance and invasive stop-and-frisk policing did not want their photographs taken by Cryptome while using the kiosk. Users seemed startled when informed that at least three onboard surveillance cameras were covertly concealed behind the kiosks' black glass.

Some users improvised solutions to temporarily alleviate the discomfort of standing at the kiosk for the duration required to fully power a rundown phone battery or to surf the web for any protracted period. Milk crates, overturned newspaper dispensers and folding chairs provide makeshift seating. Adhocked encampments of this sort will not be tolerated for long if they become extensive. Loitering laws may be invoked in certain cases as the use of the kiosk becomes more heavily policed.

NORMAL ACCIDENTS

Public health, safety and welfare (HSW) are critical criteria when considering the resiliency of lifeline infrastructures like telecom systems that have pronounced public impacts. In particular, Cryptome recognizes the complexities,

vulnerabilities and ambiguities of lifeline infrastructures,which Richard Little describes as “intricate constructions of technology, people, and governance structures.”[13]

The terrorist attacks of 9/11 underscored the characterization of New York City's iconic streets and sidewalks as high-risk environments, symbolically and materially. Asymmetric warfare and cyberwar tactics target high-value critical infrastructure that constitute the global city, including vital telecom networks and hubs. But lifeline infrastructure and large technical systems (LTS) are also vulnerable to “normal accidents” of the sort described by Charles Perrow in his research on high-risk technologies, Little notes. The organizational culture of LTS makes accidents unavoidable.

Consistent with the architect's mandate for design compliance with public health, public safety, and public welfare codes (HSW) as an ethical underpinning of professional practice, structural failure analysis is a cornerstone of the architect's training in hazard-resistant, resilient design. In this forensic spirit, Cryptome proposes the following beta-testing thought experiment for hazard resistant design remediation: what scenario would constitute a 'normal accident' within the LinkNYC system? How might a 'normal accident' produce public harm? how can this hazard be prevented?

Perrow argued complex systems predictably fail but in unpredictable ways. Human error and failures of organizational culture may be root causes. Social, political and economic factors have powerful impacts. Loss of oversight from deregulation is implicated. Observers note that market-driven neoliberal cultures optimize global grids of exchange and profit over local public safety.

Cryptome points out that civic safety is a critical goal of hazard-resistant design under the ethical framework of HSW codes. Cryptome defines civic safety as the public benefit provided by a resilient public domain that supports the material frameworks of democratic civil liberties. Civic safety cannot be surrendered as collateral damage to unpredictable normal accidents caused by failure, disruption or malfunction of the lifeline infrastructure. Violation of the material democratic space of civil liberties, including breaches that compromise personal data and metadata, or predatory capture of sidewalk performances without pedestrian awareness or consent, are examples of these. Failures may not be first order events, but secondary effects of cascading failure propagating in non-linear ways from other interconnected complex urban infrastructures, whether hazard events are man-made or natural, as Little explains.

2014 DoITT RFP

Cryptome's beta-test examines public hazards unwittingly designed into the initial requirements of NYC DoITT 2014 “Request for Proposals for a Public Communications Structures Franchise.”

1) *“Proposers are also encouraged to design the franchise structures in a way that allows components to be added in the future and existing components to be replaced. This flexibility would allow new technology to be incorporated into the franchise structures during the term of the contract, which will include an approval process for additions.”*

The above RFP stipulation underscores the risk of mission creep in LinkNYC's future. What gradual, imperceptible, unplanned shifts in the massive infrastructural system's stated objectives might evolve? Upgrades may include undisclosed sub-tenants with as yet unspecified interests who might, in future, be patched into the grid. Will some future sub-tenant be under a secrecy or non-disclosure agreement that places them beyond public oversight, against civil liberties and the public interest? Is Link currently or will it become a multi-tenant pedestal that leases space to command-and-control, or situational awareness entities operating on separate channels? Cryptome believes such pervasive, unauthorized mission creep constitutes a normal accident. Cryptome supports the public's interest in design transparency that reveals to the public any upgrades of the Link system.

A second area of interest relates to resilient design to mitigate failures that may cascade from RFP requirements for a Franchisee inventory system, as well as requirements for information tracking, sharing and data use relating to system operability:

2) *“The system will also have the capacity for contemporaneous two-way information sharing between the Department and the Franchisee regarding the installation, operation, and maintenance of the Franchise Structures. The system must be designed to capture and display information about phone and Wi-Fi operability for each installation. [Cryptome emphasis] … Proposers must include a description of the proposed computerized inventory system with its proposal describing in detail how the system will be maintained, what software will be used (“Software”) and who will be running it, and how, and for what purposes, the data contained within the system will be utilized by the Franchisee...”.*

Further: *“The franchisee will also be required to provide reports on a monthly basis showing the number, types and duration of phone calls made and the number and duration of Wi-Fi sessions per installation.”*

Franchisee inventory system, requirements for information tracking, sharing and data use relating to system operability all present challenges to civic safety. Cryptome's examination of the 2014 RFP suggest that as a matter of public health, safety and welfare – hazard-resistant design remediation is required to assure resilient civic safety in LinkNYC's lifeline infrastructure.

CONCLUSION

Our global city is a city of perpetual upgrades. Urban archaeologists remind us that 21st century fiber backbones, carrier hotels and colocation centers are built atop infrastructures of the legacy telegraph and telephony systems. Manhole covers in the streets of Manhattan and the Bronx bear the ECS logo of Empire City Subway, which since 1891 has held the franchise for what now total 11,000 manholes and 58 million feet of underground conduit -- iron pipe, vitrified clay, creosoted wood, plastic, fiberglass, concrete and currently, either 4-inch or 1.5-inch plastic ducts used in new conduit construction. Once the exclusive domain of copper wire, ECS conduits are now stuffed with TV cable and fiber.

Public utilities and monopolies have gone the way of of the dodo in the aftermath of deregulation and privatization. ECS, now a subsidiary of Verizon New York Telephone, leases conduit space to multiple providers and tenants, just as LinkNYC may lease black box space to subtenants.

Deregulation has also transformed dedicated buildings erected for telephony monopolies, like those at 60 Hudson Street, completed for Western Union in 1930, and at 32 Avenue of the Americas, completed in 1932 as headquarters for AT&T Long Lines. Today 32 AoA, a landmark of Art Deco design, is touted as "one of the key carrier neutral interconnection and co-location facilities in the world, this building offers tenants direct access to transatlantic, regional and local fiber optic networks and ISPs."

First installed in the 1880s, 25,000 model 50A coin telephones had been ordered for New York City by the end of 1912. New York City's legacy payphone cabins played a memorable character actor role in black-and-white cinema's film noir genre. The payphone cabin was the menacing site of the untraceable phone call, the blackmail threat, the anonymous ransom demand, and occasionally, the declaration of love. We'll leave it to certifiable cinephiles to draw up a listicle of the NYC payphone cubicle's top dramatic roles.

The transfer from telephone to context-aware Wi-Fi hotspot technology echoes the political context of the restructuring of Paris in the 1850s and 1860s during the Second Empire, famously directed by the prefect George-Eugène Haussmann. Robert Moses, the too-big-to-fail urban planner of mid-century's New York City's epic public works was a student of the Parisian's often ruthless tactics. Moses was a fan of the forceful way Haussman designed broad boulevards like the Champs Elysées to clear out twisting medieval streets shrewdly exploited by the revolutionary barricades of 1848.

David Harvey points out that Haussmann's boulevards were not, as is often argued, primarily strategic spaces of militarization, surveillance and control.[14] Broad boulevards indeed allowed for efficient mobilization of troops, open lines of

fire and optical surveillance of the urban population. But more important, Harvey argues, was the boulevard's role asserting proprietorship and control of urban uses for commercial purposes that favored the new consumer class. Imperial flamboyance, social displays and proliferation of department stores confirmed Paris' centrality in the circulation of money and commodities. Imperial spies and police maintained order elsewhere in the city among populations who had no rights to this emerging consumer realm.

The context-aware profilings of LinkNYC's advertising grid evoke policing procedures that enabled the restructuring of 19th century Paris as a city of money and commodities. Now as then, erotic desire entices the role of spectator and consumer into urban spectacles of consumption. But in 2016, the boulevard's access to Le Bon Marché has evolved into a matrix of online desire performed along completely connected sidewalks and streets. Automated policing and powerful command-and-control, tracking and surveillance are now built into the architecture of the spectacle.

Not everyone will be admitted to the pageant of consumption. In Paris, the term for window-shopping is “lèche-vitrine” literally: to lick the window. New Yorkers who cannot find affordable housing, a proper meal or pay for school tuition – much less access commodities advertised on 55” HD – should not be left to lick LinkNYC screens. Wet gestures anointing *lick*NYC are not likely to escape the intelligent attentive context-awareness of the kiosk's omniscient sensor array. Instead, licking the window should be understood as user generated demand for systemic transparency. Reclamation of the sidewalk into the public realm embodied by pedestrian privacy, autonomy and agency calls for such transparency through hazard-resistant design modifications to the LinkNYC system.

*** * ***

Works Consulted

1. Blackmar, Elizabeth. Appropriating “the Commons”: The Tragedy of Property Rights Discourse. in Setha M Low; Neil Smith. The politics of public space. New York : Routledge, 2006.

2. Carman, Ashley. How secure are New York City's new Wi-Fi hubs? The Verge. January 20, 2016.

3. Knutson, Ryan. New York City to Replace Pay Phones With Free Wi-Fi. The Wall Street Journal. January 5, 2016.

4. Lyon, David. Surveillance society : monitoring everyday life. Buckingham [England] ; Philadelphia : Open University Press, 2002.

5. D'Onfro, Jillian. Here's how Google's Sidewalk spinoff plans to turn your city into Tomorrowland. Business Insider. Feb. 23, 2016.

6. Waddell, Kaveh. Will New York City's Free Wi-Fi Help Police Watch You? The Atlantic. April 11, 2016.

7. Electronic Privacy Information Center. Investigations of Google Street View. https://epic.org/privacy/streetview/

8. Harris, Mark. Inside Alphabet's money-spinning, terrorist-foiling, gigabit Wi-Fi kiosks. Recode. July 1, 2016.

9. Grahame, Stephen. Cities Under Siege: The New Military Urbanism. London ; New York : Verso, 2010.

10. DeLessio, Joe. New York's New Public Wi-Fi Kiosks Are Spying on You, Says Civil-Liberties Group. New York Magazine. March 18, 2016.

11. CityBridge Privacy Policy Effective January 25, 2016 http://www1.nyc.gov/assets/doitt/downloads/pdf/Proposed-PCS-Franchise-Exhibit-2-CityBridge-Privacy-Policy.pdf

12. Request for proposals for a franchise to install, operate and maintain public communications structures in the boroughs of the Bronx, Brooklyn, Manhattan, Queens and Staten Island. PIN #8582014 FRANCH3.The City of New York Department of Information Technology and Telecommunications. http://www1.nyc.gov/assets/doitt/downloads/pdf/DoITT-Public-Communication-Structure-RFP-4-30-14.pdf

13. Little, Richard G. Managing the Risk of Cascading Failure in Complex Urban Infrastructures. in Stephen Graham, Disrupted cities: when infrastructure fails. London: Routledge, 2010.

14. Harvey, David. The Political Economy of Public Space. in Setha M Low; Neil Smith. The politics of public space. New York : Routledge, 2006.