Media and Communication

Open Access Journal | ISSN: 2183-2439

Volume 3, Issue 2 (2015)

Special Issue

Surveillance: Critical Analysis and Current Challenges (Part I)

Editors

James Schwoch, John Laprise and Ivory Mills

COGITATIO

Media and Communication, 2015, Volume 3, Issue 2
Special Issue: Surveillance: Critical Analysis and Current Challenges (Part I)

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070-129 Lisbon
Portugal

Guest Editors
James Schwoch, Northwestern University, USA
John Laprise, Independent Researcher
Ivory Mills, Northwestern University, USA

Managing Editor
Mr. António Vieira, Cogitatio Press, Portugal

Available online at: www.cogitatiopress.com/mediaandcommunication

Table of Contents

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 1-5
Doi: 10.17645/mac.v3i2.449

Editorial

Special Issue on Surveillance: Editor's Introduction

James Schwoch [1,*], John Laprise [2] and Ivory Mills [1]

[1] Department of Communication Studies and PhD Program in Media, Technology, and Society, Northwestern University, Evanston, IL 60208, USA; E-Mails: j-schwoch@northwestern.edu (J.S.), imills@u.northwestern.edu (I.M.)
[2] Independent Scholar, Des Plaines, IL 60016, USA; E-Mail: jlaprise@gmail.com

* Corresponding author

Submitted: 15 September 2015 | Published: 30 September 2015

Abstract
This Editor's Introduction discusses the interplay of surveillance issues with media and communication research.

Keywords
communication; media; surveillance

Issue
This editorial is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

On May 9, 1874, Edward Clark, the Architect of the United States Capitol, responded to U.S. House of Representatives Speaker James G. Blaine regarding questions about the telegraph offices and stations located in the corridors of the South Wing of the Capitol building.[1] Telegraph companies had established corridor offices within the Capitol to serve a range of clientele, including Congress, the Supreme Court, Library of Congress staff, additional government personnel, reporters, and visitors. Blaine had asked Clark to recommend ways in which the "telegraph instruments" could be "so isolated that it shall be impossible for any unauthorized person to hear and obtain messages." Clark consulted with Western Union and Franklin Telegraph, both of whom ran commercial telegraph offices in these corridors. He also sent J.F. Knapp, the operator of the government telegraph for the South Capitol Wing, into the field to find out where the telegrams sent by the stations in the Capitol corridors went as they left the Capitol for relay on various lines and networks. Knapp traced message flow from the Capitol up the Eastern Seaboard to Boston. He found that many messages went from the Capitol directly to the telegraph operators at the nearby Willard Hotel, and while the Willard telegraph men were considered reliable, where a telegram was relayed after that and whose hands and ears it passed through was indeterminable. Knapp, giving advice echoed by individuals from the commercial telegraph services, told Clark that "isolation" was effectively accomplished by equipping the corridor stations with two items: an ear-trumpet that captured and directed the sound of the key only to the operator's ear, and screens around the telegraph key that prevented the possibility of seeing the hand of the operator as he worked the key. Knapp called these security upgrades "silent instruments." Clark was also advised that a more secure system might mean the telegraph operator remained in public view, but with the hand on the key masked by a screen so as to be unseen by observers, because a telegraph operator in a secluded room "might allow people inside his office unobserved; whereas, situated in the corridor, the office is so public that an operator would not dare to do such a thing, as it would be too readily observed."

In other words: as best as can be accomplished in 1874 for the telegraph and the Capitol, try to find out who has access to the telegraph signal once the signal leaves the building, and in the meantime, muffle the

[1] Clark to Blaine, 9 May 1874, "Telegraph-Offices in the Corridors of the Capitol," House of Representatives, 43rd Congress, 1st session, misc. doc. 269. See annex.

sound of the telegraph key, obscure the hand of the telegraph operator, and last but not least—keep the operator in public view, constantly observed by others, to prevent the operator from divulging secrets behind closed doors. Good advice then and now, and a bit like a common social media experience today: lots of private texting going on all around you, with all the private texters in public view.

This little moment of secrecy, security, and surveillance regarding the telegraph experienced by the Architect of the Capitol of the United States of America 141 years ago may on the one hand seem comical, anachronistic, incredulous, or naive. Yet the little moment of Edward Clark also illustrates that the continual complexity and constructedness of secrecy, security, and surveillance is an ongoing process shaped by, among other things, ever-changing technological capabilities in conjunction with enduring issues about social relations, human behavior, specialized knowledge, and institutional imperatives. Media and communication research has long engaged aspects of surveillance, often related to media consumption. Circulation figures, audience ratings, phonograph record sales and hit lists, best-selling books, public opinion surveys, and letters to the editor remain a significant resource for monitoring and surveilling user consumption as well as user attitudes, while the techniques and approches to such research are now more often visible in such phenonena as music downloads, fan websites, and social media buzz. These forms of media monitoring and surveillance remain important, and are some of the examples of a long engagement of media and communication scholars with research on surveillance: propaganda; attitude formation; the scale, scope, and reach of information networks; media entertainment such feature films, radio programs, and TV shows. The ever-increasing expansion of media and communication technologies and cultures into more and more aspects of everyday global life continues as a dynamic theme of media and communication research, and surveillance is a crucial concept for understanding media and communication in the 21st century.

The Editors of this special issue are pleased to present this collection of media and communication research articles. All of the scholars in this issue are in lively and engaged pursuit of various aspects and themes of media, communication, and surveillance.

Acknowledgements

We thank the authors whose work is published herein, the editorial board and staff of *Media and Communication*, and the many external reviewers who reviewed and critiqued the manuscripts submitted for this issue.

Conflict of Interests

We declare we have no known conflicts of interest.

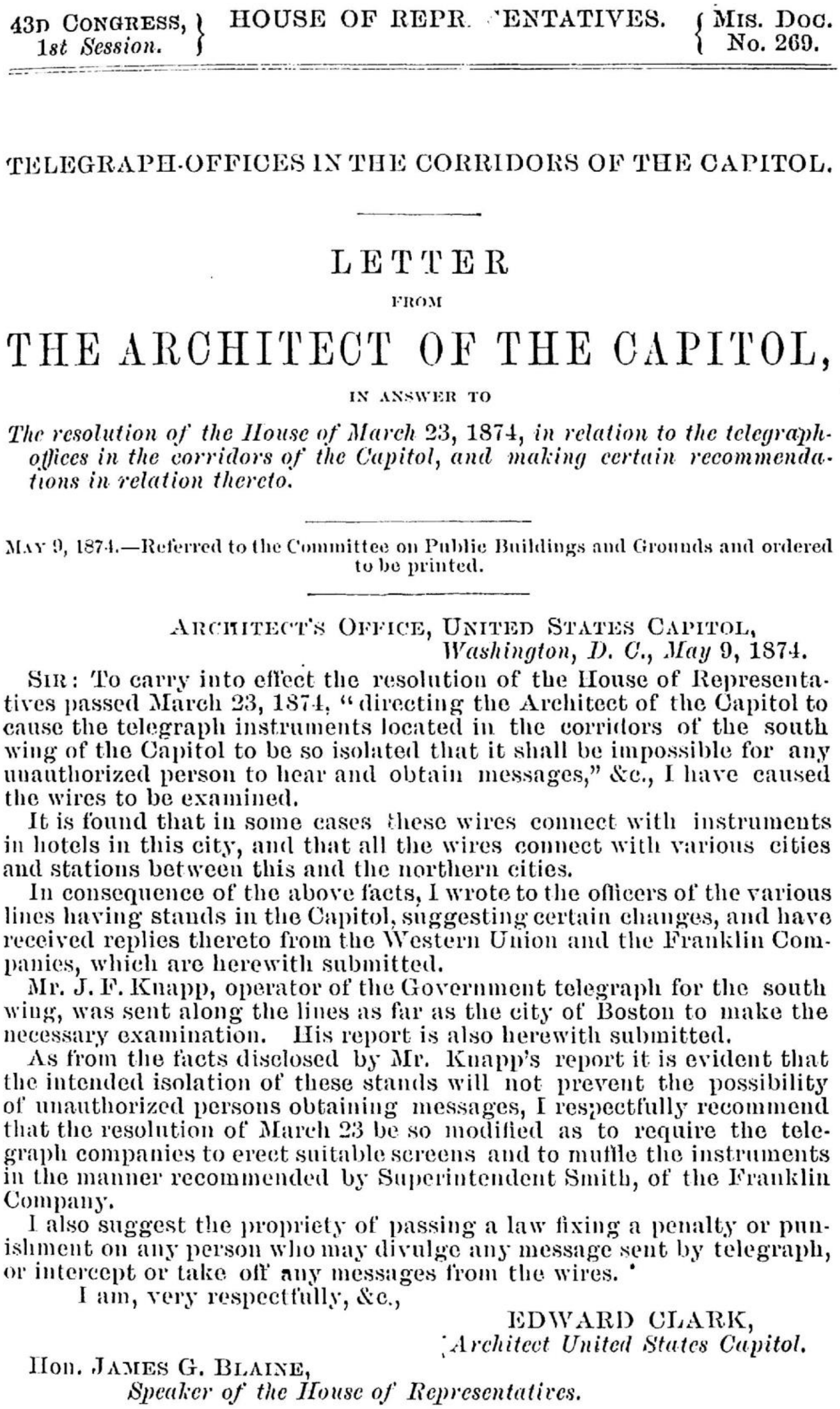
About the Authors

Dr. James Schwoch
James Schwoch is a Professor in the Department of Communication Studies and the PhD Program in Media, Technology, and Society at Northwestern University. His areas of research include global media, media history, international studies, global security, and media-communication-environment. Schwoch has published six books and many additional articles. His research has been funded by a variety of organizations. He is a member of the editorial board of *Media and Communication*.

Dr. John Laprise
John Laprise is an Independent Scholar, and was a Professor at Northwestern University's Doha, Qatar campus. His areas of research include the Internet, national security, surveillance, privacy, and technology adoption. Laprise has been a visiting scholar at the Oxford Internet Institute and a consultant to the Internet Governance Forum (IGF) under the auspices of the United Nations as well as the US IGF. His PhD is from the Media, Technology, and Society Program at Northwestern University.

Ivory Mills
Ivory Mills is a Law & Humanities Fellow and dual degree candidate at Northwestern, pursuing a PhD in Media, Technology, and Society and a JD at Northwestern Law. With interests in both theory and practice, she investigates international and comparative law and policy of ICT and telecommunications from an organizational and interorganizational perspective. Ivory holds a B.A. in International Studies from Spelman College and is a Fellow with the Institute for International Public Policy, Cohort 16.

Annex. Clark to Blaine, 9 May 1874, "Telegraph-Offices in the Corridors of the Capitol," House of Representatives, 43rd Congress, 1st session, misc. doc. 269.



43D CONGRESS, } HOUSE OF REPR. 'ENTATIVES. { MIS. DOC.
1st Session. } { No. 269.

TELEGRAPH-OFFICES IN THE CORRIDORS OF THE CAPITOL.

LETTER

FROM

THE ARCHITECT OF THE CAPITOL,

IN ANSWER TO

The resolution of the House of March 23, 1874, in relation to the telegraph-offices in the corridors of the Capitol, and making certain recommendations in relation thereto.

MAY 9, 1874.—Referred to the Committee on Public Buildings and Grounds and ordered to be printed.

ARCHITECT'S OFFICE, UNITED STATES CAPITOL,
Washington, D. C., May 9, 1874.

SIR: To carry into effect the resolution of the House of Representatives passed March 23, 1874, "directing the Architect of the Capitol to cause the telegraph instruments located in the corridors of the south wing of the Capitol to be so isolated that it shall be impossible for any unauthorized person to hear and obtain messages," &c., I have caused the wires to be examined.

It is found that in some cases these wires connect with instruments in hotels in this city, and that all the wires connect with various cities and stations between this and the northern cities.

In consequence of the above facts, I wrote to the officers of the various lines having stands in the Capitol, suggesting certain changes, and have received replies thereto from the Western Union and the Franklin Companies, which are herewith submitted.

Mr. J. F. Knapp, operator of the Government telegraph for the south wing, was sent along the lines as far as the city of Boston to make the necessary examination. His report is also herewith submitted.

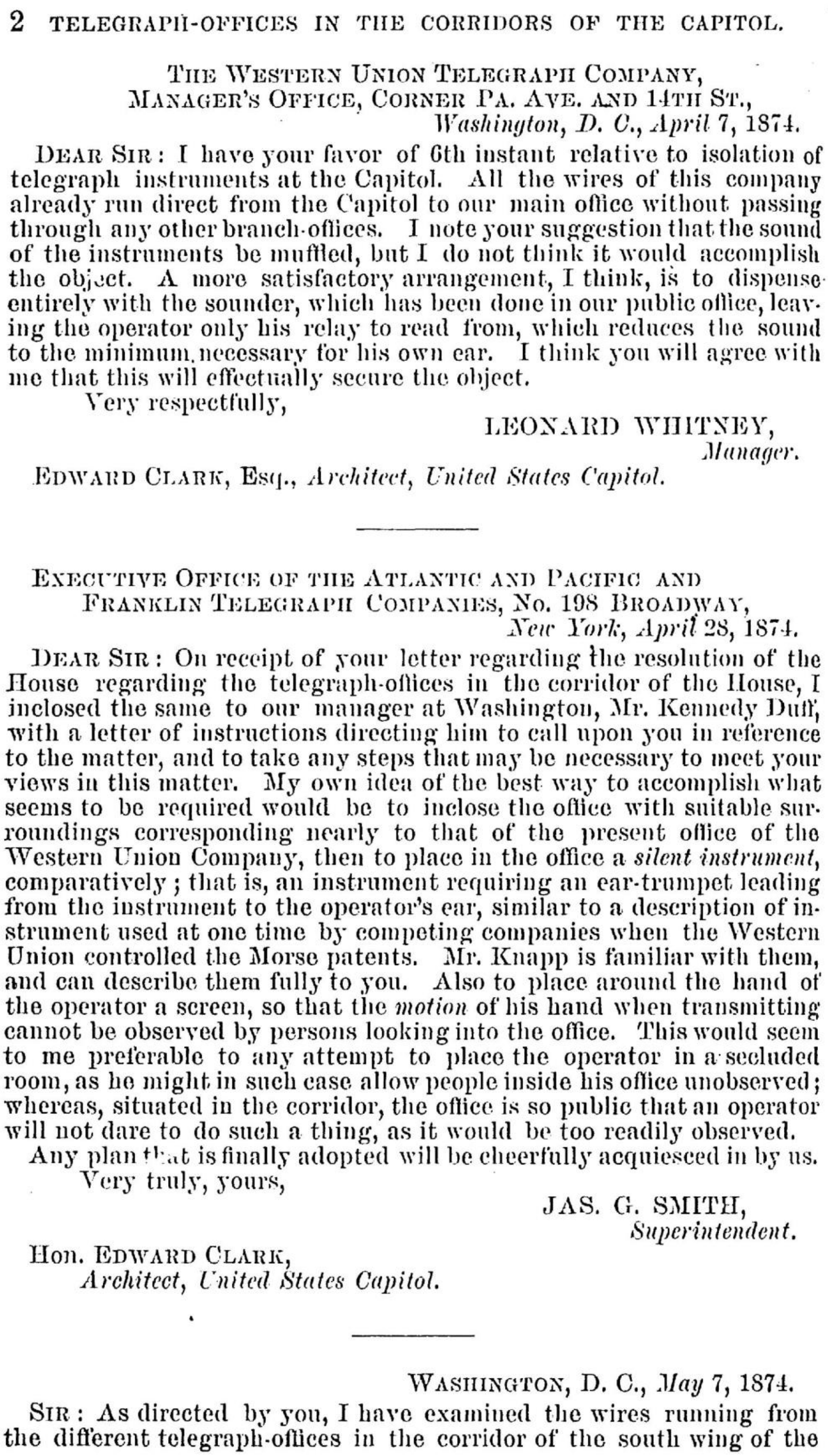
As from the facts disclosed by Mr. Knapp's report it is evident that the intended isolation of these stands will not prevent the possibility of unauthorized persons obtaining messages, I respectfully recommend that the resolution of March 23 be so modified as to require the telegraph companies to erect suitable screens and to muffle the instruments in the manner recommended by Superintendent Smith, of the Franklin Company.

I also suggest the propriety of passing a law fixing a penalty or punishment on any person who may divulge any message sent by telegraph, or intercept or take off any messages from the wires.

I am, very respectfully, &c.,

EDWARD CLARK,
Architect United States Capitol.

Hon. JAMES G. BLAINE,
Speaker of the House of Representatives.



2 TELEGRAPH-OFFICES IN THE CORRIDORS OF THE CAPITOL.

THE WESTERN UNION TELEGRAPH COMPANY,
MANAGER'S OFFICE, CORNER PA. AVE. AND 14TH ST.,
Washington, D. C., April 7, 1874.

DEAR SIR: I have your favor of 6th instant relative to isolation of telegraph instruments at the Capitol. All the wires of this company already run direct from the Capitol to our main office without passing through any other branch-offices. I note your suggestion that the sound of the instruments be muffled, but I do not think it would accomplish the object. A more satisfactory arrangement, I think, is to dispense entirely with the sounder, which has been done in our public office, leaving the operator only his relay to read from, which reduces the sound to the minimum necessary for his own ear. I think you will agree with me that this will effectually secure the object.

Very respectfully,

LEONARD WHITNEY,
Manager.

EDWARD CLARK, Esq., *Architect, United States Capitol.*

EXECUTIVE OFFICE OF THE ATLANTIC AND PACIFIC AND
FRANKLIN TELEGRAPH COMPANIES, No. 198 BROADWAY,
New York, April 28, 1874.

DEAR SIR: On receipt of your letter regarding the resolution of the House regarding the telegraph-offices in the corridor of the House, I inclosed the same to our manager at Washington, Mr. Kennedy Duff, with a letter of instructions directing him to call upon you in reference to the matter, and to take any steps that may be necessary to meet your views in this matter. My own idea of the best way to accomplish what seems to be required would be to inclose the office with suitable surroundings corresponding nearly to that of the present office of the Western Union Company, then to place in the office a *silent instrument*, comparatively; that is, an instrument requiring an ear-trumpet leading from the instrument to the operator's ear, similar to a description of instrument used at one time by competing companies when the Western Union controlled the Morse patents. Mr. Knapp is familiar with them, and can describe them fully to you. Also to place around the hand of the operator a screen, so that the *motion* of his hand when transmitting cannot be observed by persons looking into the office. This would seem to me preferable to any attempt to place the operator in a secluded room, as he might in such case allow people inside his office unobserved; whereas, situated in the corridor, the office is so public that an operator will not dare to do such a thing, as it would be too readily observed.

Any plan that is finally adopted will be cheerfully acquiesced in by us.

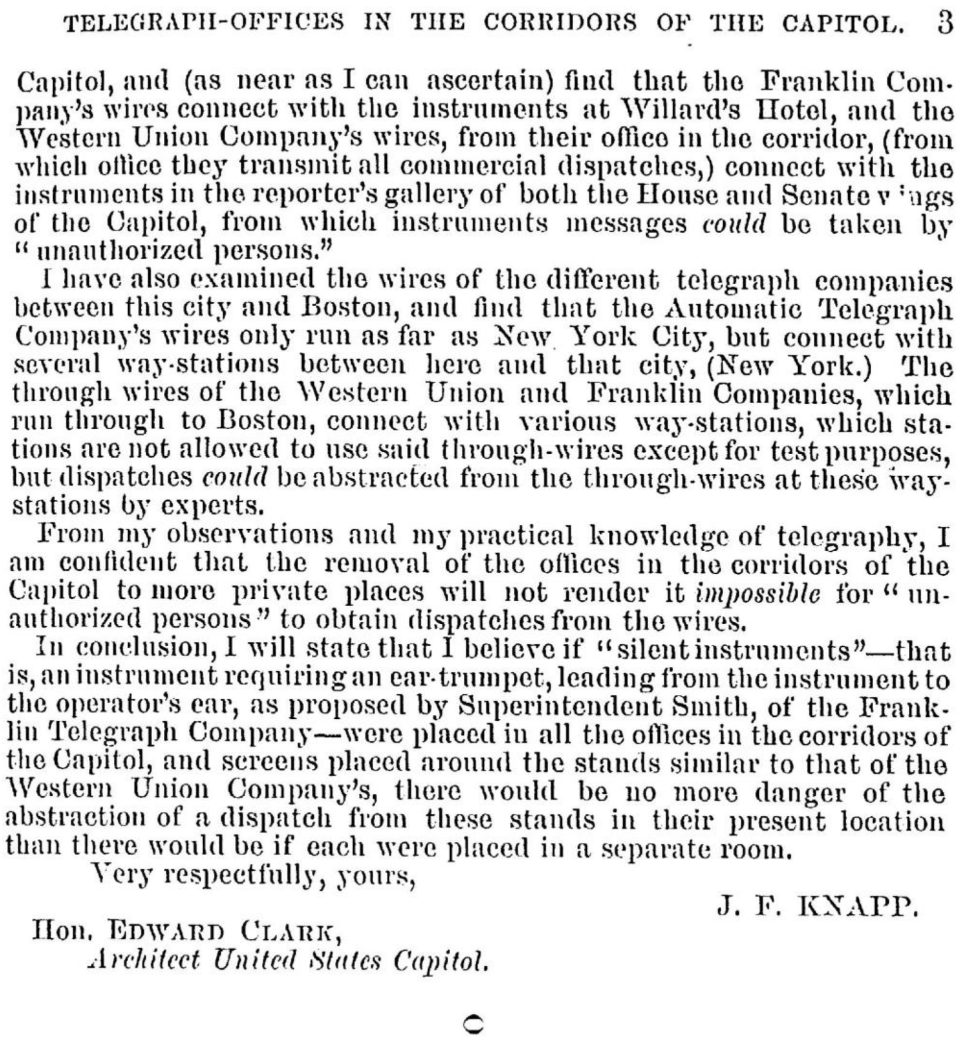
Very truly, yours,

JAS. G. SMITH,
Superintendent.

HON. EDWARD CLARK,
Architect, United States Capitol.

WASHINGTON, D. C., *May* 7, 1874.

SIR: As directed by you, I have examined the wires running from the different telegraph-offices in the corridor of the south wing of the



TELEGRAPH-OFFICES IN THE CORRIDORS OF THE CAPITOL. 3

Capitol, and (as near as I can ascertain) find that the Franklin Company's wires connect with the instruments at Willard's Hotel, and the Western Union Company's wires, from their office in the corridor, (from which office they transmit all commercial dispatches,) connect with the instruments in the reporter's gallery of both the House and Senate wings of the Capitol, from which instruments messages *could* be taken by "unauthorized persons."

I have also examined the wires of the different telegraph companies between this city and Boston, and find that the Automatic Telegraph Company's wires only run as far as New York City, but connect with several way-stations between here and that city, (New York.) The through wires of the Western Union and Franklin Companies, which run through to Boston, connect with various way-stations, which stations are not allowed to use said through-wires except for test purposes, but dispatches *could* be abstracted from the through-wires at these way-stations by experts.

From my observations and my practical knowledge of telegraphy, I am confident that the removal of the offices in the corridors of the Capitol to more private places will not render it *impossible* for "unauthorized persons" to obtain dispatches from the wires.

In conclusion, I will state that I believe if "silent instruments"—that is, an instrument requiring an ear-trumpet, leading from the instrument to the operator's ear, as proposed by Superintendent Smith, of the Franklin Telegraph Company—were placed in all the offices in the corridors of the Capitol, and screens placed around the stands similar to that of the Western Union Company's, there would be no more danger of the abstraction of a dispatch from these stands in their present location than there would be if each were placed in a separate room.

Very respectfully, yours,

J. F. KNAPP.

Hon. EDWARD CLARK,
Architect United States Capitol.

○

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 6-9
Doi: 10.17645/mac.v3i2.207

Commentary

Surveillance and Critical Theory

Christian Fuchs

Communication and Media Research Institute, University of Westminster, Middlesex, HA1 3TP, UK;
E-Mail: christian.fuchs@uti.at

Submitted: 8 November 2014 | Accepted: 27 November 2014 | Published: 30 September 2015

Abstract
In this comment, the author reflects on surveillance from a critical theory approach, his involvement in surveillance research and projects, and the status of the study of surveillance. The comment ascertains a lack of critical thinking about surveillance, questions the existence of something called “surveillance studies” as opposed to a critical theory of society, and reflects on issues such as Edward Snowden’s revelations, and Foucault and Marx in the context of surveillance.

Keywords
critical theory; Edward Snowden; Karl Marx; Michel Foucault; surveillance

Issue
This commentary is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

I have since 2008 been active in research networks and involved in one nationally funded and two EU-funded research projects on surveillance. I have worked with PhD students and postdocs on the topic of surveillance, have written multiple articles and chapters, and have edited books on surveillance in general as well as digital surveillance in particular. In this comment, I reflect on the relationship of surveillance and critical theory and my experiences in studying surveillance.

There has been surprisingly little use of Karl Marx and the Frankfurt School’s works for studying surveillance and privacy. There have been some exceptions, such as the works by Oscar Gandy, Thomas Mathiesen, and studies inspired by Harry Braverman’s labour process theory. Studies of surveillance tend to see Marx only as relevant for understanding the surveillance of workers or neglect Marx and Marxist theory altogether with the well-known (and false) argument that his works are outdated (see: Fuchs & Mosco, 2012; Fuchs, 2014a). When I started research on surveillance, I set myself as one of the tasks to conduct studies that explore the relationship of capitalist society and surveillance. It is important to see that Marx and Marxism matter in this respect not just for understanding economic surveillance, but also for explaining the connection of surveillance with the modern state, media and technology, ideologies, hegemony, class struggles, and alternatives to surveillance society (see for example: Allmer, Fuchs, Kreilinger, & Sevignani, 2014; Fuchs, 2011a, 2011b, 2011c, 2012a, 2012c, 2012d, 2013a; Fuchs, Boersma, Albrechtslund, & Sandoval, 2012; Fuchs & Mosco, 2012; Fuchs & Trottier, 2013, forthcoming a, Trottier & Fuchs, 2015). The modern economy and the modern state depend on the control of workers, consumers, prosumers, and citizens. Surveillance is a form of domination that is an inherent feature of capitalism.

For grounding a critical theory of privacy and surveillance, I have found it interesting to explore the relationship of Marx and Foucault (see for example: Fuchs, 2013a; Fuchs, 2011a). The notions of control, power, and surveillance are an obvious point of departure. It should also be seen that Foucault (2008) introduced his notion of governmentality in a profound study of the 20th century’s political economic theory and the rise of neo-liberalism. In contemporary studies of surveillance, Foucault does surprisingly not occupy a dominant but a minority position. Many scholars hold the position that the notion of panoptic surveillance is outdated because it presupposes a surveillant centre that monitors the many. The rise of new technologies, especially the Internet, would have decentralised surveillance and given rise to a democratisation of surveillance in which the many monitor those in power ("participatory surveillance"). Although subordinate groups can and do make use of digital technologies for surveilling the surveillors to a certain degree, the state and capitalists have much more resources than civil society and citizens, which enables them to conduct much more intensive and extensive forms of surveillance. They make use of decentralised surveillance for centralising surveillant, economic, and political power. The NSA monitors your use of Google and Facebook, but you do not monitor the NSA agent monitoring you, which shows a fundamental power asymmetry. Capital and the state are as collective actors the dominant surveillors. Notions such as the surveillant assemblage and participatory surveillance are relativist and downplay the actual repressive power of capitalism and the state.

"Surveillance studies" claims to be a new interdisciplinary field of research, teaching, and studies. It shares this claim with other new self-proclaimed inter-/multi-/trans-/anti-disciplines such as science and technology studies (STS), Internet research, social media studies/research, social informatics, information science, web studies, systems theory/cybernetics, digital humanities, etc. Such claims serve the mere purpose of accumulating academic resources in the competition for research money, students, academic positions, departments and institutions, journals, publications, citations, etc. with other fields. Although disguised as being inter- and transdisciplinary, the "new" trans- and interdisciplines are the new disciplines that share the same kind of power play with older fields and disciplines and thereby do not question, but reproduce the academic field's logics of power and accumulation. They are not new, but old in their conservative reproduction and uncritical acceptance of academia's power structures. I have found such claims and struggles for new fields completely pointless because the only thing that matters really is being a critical researcher, whereas one should not give a damn about identifying oneself as social researcher, media and communication researcher, surveillance researcher, computer scientist, or something different.

Disciplinary box thinking is an evil that needs to be overcome. Critical theory is the only effective means that can be used for this purpose. Max Horkheimer (1931) understood critical theory as a truly interdisciplinary and holistic project that brings together various researchers from different backgrounds that study society as a whole so that power structures, class, authority, and domination are investigated in a manner that creates a better understanding that can contribute to the establishment of a non-instrumental society that fosters the public good, happiness and wealth for all. Critical research has under neoliberal conditions been rendered minoritarian. The struggle for new in/disciplines is part of the attempted neoliberalisation of (almost) everything.

In "surveillance studies", key proponents of the institutionalisation as a discipline have followed the strategy to inflate the object of study in order to make the claim that it is large enough for giving grounds to the formation of a new discipline that sees itself as being interdisciplinary. This has resulted in an uncritical, positivistic, and overgeneral understanding of surveillance (Fuchs, 2011a). In contrast to Foucault, many surveillance scholars define surveillance as the collection of information for attaining a specific purpose and say that surveillance is not automatic positive or negative. A Nazi henchman monitoring Jews in Auschwitz who are sent to the gas chamber on the next day is in this administrative understanding equated on the same definitional level with a babyphone that monitors a sleeping baby, an electrocardiogram, or an earthquake detection system considered as constituting forms of surveillance. Such a concept of surveillance is not only completely useless for a critical theory, but also politically dangerous. For countering this tendency, we need a purely negative concept of surveillance, in which surveillance is a specific form of control that forms one dimension of domination, exploitation, class, capitalism, patriarchy, racism, and similar negative phenomena (Fuchs, 2011a). Just like Adorno (1973/2003) was calling for a negative dialectic, we need based on Foucault and Marx negative surveillance studies. A problem of the general understanding of surveillance is also that it makes surveillance categorically synonymous with information collection and processing so that no differentiation can be drawn between surveillance theory and information theory.

Edward Snowden revealed in 2013 the existence of global Internet surveillance systems such as Prism, XKeyScore, or Tempora that are operated in collaborations of secret services and capitalist communications companies. Hundreds of research projects focusing on privacy and surveillance could not uncover the existence of this surveillance-industrial Internet complex for the simple fact that surveillance power tends to be invisible and secret and it is difficult to challenge and investigate intransparent power. Institutions such as the European Union fund the development of new surveillance technologies with hundreds of millions Euros, whereas the funding of critical, societal, and ethical impact assessment of information technologies is something quite new and is trapped in the contradiction that such researchers find themselves put into large consortia with representatives of the surveillance-industrial complex, who bring a conservative law and order position to projects that limits and biases research. Snowden's revelations also made once and for all clear how conceptually wrong those who talk about a democratisation of surveillance and the emergence of "participatory surveillance" actually are. In the surveillance-industrial complex, the world's most powerful state institutions have collaborated with the world's most powerful communications companies to implement totalitarian surveillance systems. It is a system that centralises control by monitoring decentralised technologies with multiple technologies and networking the obtained data. The result is centralised surveillance that as whole is a sum that is larger than its parts.

Because there are citizens in the world who care about a better world, we fortunately have attempts to hold the powerful accountable with the help of WikiLeaks, whistleblowing, investigative journalism, corporate watch platforms, alternative media, etc. The problem that critical citizens and critical media projects however face is that they often lack resources, visibility, attention, and power. They are in a minoritarian position and face power asymmetries that are constituted by the networked power of military, state and capitalist institutions. Surveillance is contested, but in the associated social struggles civil society and social movements are automatically disadvantaged in terms of resources and political economy.

The rise of so-called social media has resulted in a new round of techno-optimism. Ideologues, politicians, management gurus, uncritical scholars, capitalists and their interest organisations, as well as a specific share of citizens, consumers, and users who uncritically accept the discourse that the new is always something better have argued that social media brings about political revolutions, creates employment, wealth for all, a new public sphere, participatory organisations, better democracies, etc. But in contrast to such claims, for example recent rebellions and revolutions have not been Twitter and Facebook revolutions. Rather there is a complex dialectic of offline and online action, mediated and face-to-face communication in such forms of collective political action (Fuchs, 2014c). In addition the positive vision has been proven wrong by the privacy implications of social media capital accumulation models that use in-built real time surveillance and the exploitation of digital labour (Fisher & Fuchs, 2015, Fuchs, 2014a, 2014b, 2015; Fuchs & Sandoval, 2014; Sandoval, Fuchs, Prodnik, Sevignani, & Allmer, 2014), Snowden's revelations (Fuchs & Trottier, forthcoming b), and Western capitalist communications companies' exports of surveillance technologies to regimes that use these tools for monitoring activists who as a consequence have been threatened, tortured, and repressed (Fuchs, 2013b; Fuchs, 2012b).

In order to adequately understand the Internet, media, communications, and surveillance, we need a critical theory of society for the 21st century. Critical theory is a crucial tool that based on its long history and new developments in society, communications, and theory can create systematic knowledge that can support struggles for a humane society—a society without domination and without surveillance.

Conflict of Interests

The author declares no conflict of interests.

References

Adorno, T. W. (2003). *Negative dialectics*. London: Routledge. (Original work published 1973)

Allmer, T., Fuchs, C., Kreilinger, V., & Sevignani, S. (2014). Social networking sites in the surveillance society: Critical perspectives and empirical findings. In A. Jansson & M. Christensen (Eds.), *Media, surveillance and identity. Social perspectives* (pp. 49-70). New York: Peter Lang.

Fisher, E., & Fuchs, C. (2015). Reconsidering value and labour in the digital age. In U. Huws & R. Gill (Eds.), *Dynamics of virtual work* (Vol. 1). Basingstoke: Palgrave Macmillan.

Foucault, M. (2008). *The birth of biopolitics*. Basingstoke: Palgrave Macmillan.

Fuchs, C. (2011a). How to define surveillance? *MATRIZes*, *5*(1), 109-133.

Fuchs, C. (2011b). New media, web 2.0 and surveillance. *Sociology Compass*, *5*(2), 134-147.

Fuchs, C. (2011c). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4), 220-237.

Fuchs, C. (2012a). Critique of the political economy of web 2.0 surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance. The challenges of web 2.0 and social media* (pp. 31-70). New York: Routledge.

Fuchs, C. (*2012b). Implications of deep packet inspection (DPI) Internet surveillance for society* (The Privacy & Security Research Paper Series #1). Rome: Centre for Science, Society & Citizenship. Retrieved from http://fuchs.uti.at/wp-content/uploads/DPI.pdf

Fuchs, C. (2012c). The political economy of privacy on Facebook. *Television & New Media*, *13*(2), 139-159.

Fuchs, C. (2012d). Web 2.0 surveillance and art. In X. Burrough (Ed.), *Net works: Case studies in web art and design* (pp. 121-127). New York: Routledge.

Fuchs, C. (2013a). Political economy and surveillance theory. *Critical Sociology*, *39*(5), 671-687.

Fuchs, C. (2013b). Societal and ideological impacts of deep packet inspection (DPI) Internet surveillance. *Information, Communication and Societ*y, *16*(8), 1328-1359.

Fuchs, C. (2014a). *Digital labour and Karl Marx.* New York: Routledge.

Fuchs, C. (2014b). *Social media: A critical introduction.* London: Sage.

Fuchs, C. (2014c). *OccupyMedia! The occupy movement* *and social media in crisis capitalism.* Winchester: Zero Books.

Fuchs, C. (2015). *Culture and economy in the age of social media.* New York: Routledge.

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.). (2012). *Internet and surveillance. The challenges of web 2.0 and social media.* New York: Routledge.

Fuchs, C., & Mosco, V. (Eds.). (2012). Marx is back—The importance of Marxist theory and research for critical communication studies today. *Triple—Open Access Journal for a Global Sustainable Information Society*, *10*(2), 127-632.

Fuchs, C., & Trottier, D. (2013). The internet as surveilled workplayplace and factory. In S. Gutwirth, R. Leenes, P. De Hert, & Y. Poullet (Eds.), *European data protection. Coming of age* (pp. 33-57). Dordrecht: Springer.

Fuchs, C., & Sandoval, M. (Eds.). (2014). *Critique, social media & the information society*. New York: Routledge.

Fuchs, C., & Trottier, D. (forthcoming a). Towards a theoretical model of social media surveillance in contemporary society. *Communications—The European Journal of Communication Research*.

Fuchs, C., & Trottier, D. (forthcoming b). How do computer and data experts think about internet surveillance in the age of Edward Snowden?

Horkheimer, M. (1931). The state of contemporary social philosophy and the tasks of an institute for social research. In S. E. Bronner & D. Kellner (Eds.), *Critical theory and society. A reader* (pp. 25-36). New York: Routledge.

Sandoval, M., Fuchs, C., Prodnik, J. A., Sevignani, S., & Allmer, T. (Eds.). (2014). Philosophers of the world unite! Theorising digital labour and virtual work. *TripleC: Communication, Capitalism & Critique, 12*(2), 464-801.

Trottier, D., & Fuchs, C. (Eds.) (2015). *Social media, politics, and the state. Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube*. New York: Routledge.

About the Author

Dr. Christian Fuchs

Christian Fuchs is Professor at and Director of the University of Westminster's Communication and Media Research Institute (CAMRI). He is editor of the open access *journal tripleC: Communication, Capitalism & Critique* (http://www.triple-c.at) and author of many publications in the fields of critical theory and critical political economy of communications and digital media.

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 10-20
Doi: 10.17645/mac.v3i2.251

Article

Theorizing Surveillance in the UK Crime Control Field

Michael McCahill

School of Social Science, University of Hull, Hull, HU67RX, UK; E-Mail: M.McCahill@hull.ac.uk

Submitted: 24 February 2015 | In Revised Form: 8 July 2015 | Accepted: 23 July 2015 |
Published: 30 September 2015

Abstract

Drawing upon the work of Pierre Bourdieu and Loic Wacquant, this paper argues that the demise of the Keynesian Welfare State (KWS) and the rise of neo-liberal economic policies in the UK has placed new surveillance technologies at the centre of a reconfigured "crime control field" (Garland, 2001) designed to control the problem populations created by neo-liberal economic policies (Wacquant, 2009a). The paper also suggests that field theory could be usefully deployed in future research to explore how wider global trends or social forces, such as neo-liberalism or bio-power, are refracted through the crime control field in different national jurisdictions. We conclude by showing how this approach provides a bridge between society-wide analysis and micro-sociology by exploring how the operation of new surveillance technologies is mediated by the "habitus" of surveillance agents working in the crime control field and contested by surveillance subjects.

Keywords

capital; crime control; resistance; surveillance

Issue

This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction

Surveillance, defined as the "collection and analysis of information about populations in order to govern their activities" (Haggerty & Ericson, 2006, p. 3), has always been a central feature of policing and criminal justice. This includes the "direct supervision" of subject populations in prisons and probation work and the accumulation of "coded information" (Giddens, 1985) which began in the nineteenth century when fingerprints, photographs and files were collated by criminal justice practitioners. Over the last two decades however the advent of computer databases, surveillance cameras and other technological advances are said to have given rise to a "new surveillance"[1] (Marx, 2002) comprising of "surveillant assemblages" (Haggerty & Ericson, 2000) which operate well beyond the confines of the central state. In an attempt to make sense of these developments, the theoretical literature has been dominated by Foucaultian and Deleuzian-inspired perspectives on "discipline" (Foucault, 1977) and "control" (Deleuze, 1992). As Lyon (1993, p. 655) points out, for many writers "the idea of exploiting uncertainty in the observed as a way of ensuring their subordination has obvious resonance with current electronic technologies that permit highly unobtrusive monitoring of data subjects in a variety of social contexts". For other writers, the disciplinary model of surveillance eventually proved too inflexible "to organize the mobile labour forces and financial flows of complex information economies" (Bogard, 2012, p. 33). Thus, while for some writers the emergence of new surveillance technologies is consistent with the "disciplinary power" and "self-governing capabilities" identified by Foucault (Staples & Decker, 2008), for others disciplinary power has been replaced with "modulation" which works through models, simulation, codes, statistical tracking, and new methods of social sorting (Bogard, 2012, pp. 32-33).

[1] For Gary T. Marx (2002, p. 12), new surveillance refers to "the use of technical means to extract or create personal data".

The central argument presented here is that the Focuaultian and Deleuzian-inspired literature outlined above does not adequately address the *politics of surveillance* by explaining why or how new surveillance technologies have come to play such a central role in contemporary society and in particular how they have become central to policing and criminal justice. As Haggerty (2006, p. 34) points out, in the Foucualtian literature, "the movement of panoptic principles into new settings" is "often presented as entirely frictionless" and lacking any "sense of a surveillance politics". Similarly, Deleuzian-inspired accounts of the emergence of networked and flexible forms of control in response to the global system of capital (Bogard, 2006) operate at a very high level of abstraction and consequently fail to explore how wider global trends or social forces, such as neo-liberalism or bio-power, are refracted through the crime control field in different national jurisdictions. To address these questions, we situate the emergence of new surveillance technologies within "fields of struggle", defined by Bourdieu "as a structured space of positions in which the positions and their interrelations are determined by the distribution of different kinds of resources or "capital" (Thompson, 1991, p. 14). We begin at the macro level by showing how globalizing forces and wider social changes are filtered through the "field of power"[2] in different national jurisdictions. Next, we argue that the demise of the Keynesian Welfare State (KWS) and the rise of neo-liberal economic policies in the UK has placed new surveillance technologies at the centre of a reconfigured "crime control field" (Garland, 2001) designed to control the problem populations created by neo-liberal economic policies (Wacquant, 2009a). Finally, we show how field theory provides a bridge between society-wide analysis and micro-sociology by showing how the operation of new surveillance technologies is mediated by the "*habitus*"[3] of surveillance agents and surveillance subjects. But first we explain how and why we intend to use this approach to make sense of contemporary developments.

2. Why "Field" Theory?

In an early paper entitled, "The Genesis of the Bureaucratic Field", Pierre Bourdieu (1984) extends Max Weber's definition of the state as an institution "which possesses a monopoly over the legitimate use of (physical) violence", by adding that the bureaucratic field "also monopolizes the use of 'symbolic violence'" (Benson, 2005, p. 93). For Bourdieu, symbolic violence is the power to "constitute the given" (Bourdieu, 1991, p. 170) and refers to the state's "ability to make appear as natural, inevitable, and thus apolitical, that which is a product of historical struggle and human invention" (Loveman, 2005, p. 1655). From this perspective, the development of bureaucratic administration and the use of "civil registration and related forms of state identification of individuals are at the core of modern states' capacity to exercise symbolic power" (Loveman, 2005, p. 1679). In this respect, Bourdieu's early paper on the state complements the work of other social theorists who have documented how surveillance originally emerged in the context of state bureaucracy, policing and government administration (Dandeker, 1990; Lyon, 1994). However, while Bourdieu used field theory to explore a wide-range of semi-autonomous and increasingly specialized spheres of action, such as the fields of politics, religion, and cultural production, he did not write about the "crime control field" (Garland, 2001) which makes up a key component of the "right hand of the state" (Wacquant, 2009a, p. 289; see also Page, 2013), nor did he have anything to say about the emergence of a "surveillance society" which has seen surveillance proliferate well beyond the bureaucratic field to become a routine and mundane feature that is "embedded in every aspect of life" (Lyon, 2001, p. 1). In recent years however a number of writers have used field theory to analyse penal transformation in the age of neo-liberalism. Didier Bigo (2000, 2002), for example, has outlined the emergence of a transnational field of security professionals across the European Union involved in the "management of unease" (Bigo, 2002, p. 64). This approach has also been used by Dupont (2004, p. 85) who draws upon Bourdieu's notion of "capitals" (economic, social, cultural and symbolic) to explore how these resources can be "used as strategic assets to acquire or maintain a dominant position within security networks". Garland (2001) meanwhile combines "field" theory with "governmentality" (Foucault, 1991) to argue that recent transformations in policing, punishment, sentencing and crime prevention "can best be grasped by viewing them as interactive elements in a structured field of crime control and criminal justice" (Garland, 2001, p. x). Finally, Wacquant (2009) has drawn upon Bourdieu's distinction between the "left hand" of the state (e.g. education, health, social assistance) and the "right hand" of the state (e.g. police, justice, and correctional administrations) (Bourdieu, 1998, p. 2) to examine the fusion of penal policy and welfare policy to manage the problem populations generated by neo-liberal economic policies.

One of the recurring criticisms levelled at Bourdieu's writings on the "bureaucratic field" is that he tends to generalise from the case of the (strong and centralised) French state and consequently "fails to speak to those in the Anglophone world who have ex-

[2] The "field of power" refers to "the upper reaches of the social class structure where individuals and groups bring considerable amounts of various kinds of capital into their struggles for power" (Swartz, 2004, p. 12).

[3] Habitus refers to the "set of *dispositions* which incline agents to act and react in certain ways" (Thompson, 1991, p. 12).

perienced over thirty years of the rolling back of the state by neo-liberal governments" (A. Scott, 2013, p. 65). From this perspective, notions of "nodal governance" (Johnston & Shearing, 2003) or "governmentality" (Foucault, 1991) are much more suitable for theorizing the emergence of "surveillant assemblages" (Haggerty & Ericson, 2000) which operate beyond the confines of the bureaucratic field. However, following A. Scott (2013), we argue that it possible to use Bourdieu's parochialism (regarding his generalisation from the "strong" French state) to counter our own (Anglophone) parochialism regarding the "weak" neo-liberal state (A. Scott, 2013). In this respect, Bourdieu's writings on the bureaucratic field provide a means of critically engaging with the Foucaultian and Deleuzian literature which underestimates how neo-liberal strategies of privatization can serve to strengthen the position of political elites (A. Scott, 2013). From this perspective, law and order campaigns and the introduction of new laws and surveillance measures "reassert the authority of the state and shore up the deficit of legitimacy officials suffer when they abandon the mission of social and economic protection established during the Fordist-Keynesian era" (Wacquant, 2010, p. 198). At the same time, this approach avoids economic reductionism or conspiracy theory[4], focusing instead on how social fields emerge as the result of on-going struggles between actors whose aim is to set "the rules that govern the different social games (fields) and, in particular, the rules of reproduction of these games" (Wacquant, 1993, p. 42).

The use of field theory outlined above we argue provides a useful theoretical framework for examining the *politics of surveillance* in the UK crime control field. However, there are two caveats to our use of this approach to theorize current surveillance practice. Firstly, while much of the criminological literature has focused on state surveillance and policing, this is too restrictive for an analysis of the new surveillance which increasingly operates across state and non-state institutions. To avoid this limitation we use Garland's (2001) broader definition of the "crime control field". This includes "the formal controls exercised by the state's criminal justice agencies and the informal social controls that are embedded in everyday activities and interactions in civil society" (2001, p. 5). This more expansive conception of the crime control field allows us to examine the social impact of new surveillance in both the penal sector of the bureaucratic field (e.g. prisons, probation and policing) and in the wider society which has seen new surveillance measures introduced in schools, universities, shopping malls, airports etc. (Simon, 2007). Secondly, the question of how those on the receiving end of surveillance experience and respond to being monitored has received relatively little attention (although see Marx, 2003). For instance, in his account of how penal sanction and welfare supervision have merged "into a single apparatus for the cultural capture and behavioural control of marginal populations", Wacquant (2009a, p. xix) explains how his approach "does not survey efforts to resist, divest, or divert the imprint of the penal state from below". To address this issue we draw upon recent ethnographic research designed to explore how a diverse range of groups experience and respond to being monitored by the new surveillance technologies that are currently used in the crime control field (McCahill & Finn, 2014). We situate the emergence of surveillance within "fields of struggle", arguing that the distribution of various forms of "capital"—economic, social, cultural and symbolic—operate as a range of goods or resources that structure the dynamics of surveillance practices and power relations in the crime control field. By doing this we also extend Bourdieu's conceptual toolkit by introducing the term *surveillance capital* to illustrate how surveillance subjects utilise everyday forms of cultural know-how acquired through first-hand experience of power relations to challenge the very same power relations. However, before we examine the micro-politics of resistance, we need to situate the emergence of new surveillance in a wider political context.

3. The Global Diffusion of Surveillance—The Case of CCTV Surveillance Cameras

As Murakami Wood (2009, p. 181) has argued, generalised descriptions of a surveillance society often underplay the "immense cultural and geographic variety of surveillance *societies*" (emphasis added). Bourdieu's work is useful here because he "explodes the vacuous notion of 'society' and replaces it with those of field and social space". For Bourdieu, "fields of struggle" are relatively autonomous social spaces "that cannot be collapsed under an overall societal logic" (Bourdieu & Wacquant, 1992, p. 17) such as "modernity" or "postmodernity", or, we might add, the "surveillance society". Globalizing forces and wider social change, for example, are always filtered through the political and juridical fields of different national jurisdictions. Comparative work conducted by criminologists on the uneven global diffusion of the "new punitiveness[5] may

[4] As Bigo (2000) has argued in the context of the emergence of a European security field, "there is no cabal—be it based within a faction of politicians, or of police officials, or both—conspiring to undermine civil liberties and increase the powers of police agencies. Rather, a field has emerged which is the result of on-going struggles between actors" (Bigo, 2000, p. 90).

[5] As Nelken (2005, pp. 220-221) points out, while new surveillance "cannot be classified as 'stigmatizing punishments'…there would be a strong argument for taking them into account in terms of the way they tend to replace expenditure on more "social" forms of prevention, and the

be useful here for exploring the diffusion of new surveillance. For instance, in their comparative study of criminal justice in twelve different countries, Cavadino and Dignan (2006) constructed a typology of political economy which showed major differences between neo-liberal (USA, South Africa, England and Wales, Australia, New Zealand), conservative-corporatist (Germany, France, Italy, and the Netherlands), social democratic (Sweden and Finland), and oriental-corporatist countries (Japan). In short, they found that neo-liberal countries were more punitive (exhibiting higher prison rates, lower age of criminal responsibility, and adoption of privatization policies), followed by conservative corporatist, social democratic and oriental corporatist (in Lacey, 2008, pp. 44-45). These findings have been supported by Lacey (2008) in her "comparative institutional analysis" which showed that Liberal Market Economies (LMEs) (especially the UK and USA) adopted more exclusionary criminal justice systems than Coordinated Market Economies (CMEs) (north-western Europe, Scandinavia and Japan).

Any attempt to address similar questions in relation to the global diffusion of new surveillance would require systematic comparative research. However, there are one or two studies that allow us to raise some tentative questions or hypotheses that may guide future research. For instance, while research conducted on the rise of CCTV surveillance in Europe by the Urbaneye project found a general diffusion of surveillance cameras throughout European society, the growth of these systems in countries such as Germany and Norway was restricted due to the contrasting legal and constitutional environments of the juridical fields (see Norris, McCahill, & Murakami Wood, 2004, p. 121). Thus, while the legal context in the UK is extremely permissive, privacy rights in CMEs such as Denmark and Norway are constitutionally enshrined. The latter also have strong data protection regimes to regulate the introduction and use of new surveillance measures such as CCTV surveillance cameras (see Norris et al., 2004, p. 121). The uneven proliferation of "new surveillance" must also be situated in a wider socio-economic context. Thus, whereas CMEs are "premised on incorporation" and "the need to reintegrate offenders onto society and economy", LMEs are based on flexibility and innovation which means that "under conditions of surplus unskilled labour…the costs of a harsh, exclusionary criminal justice system are less than they would be in a co-ordinated market economy" (Lacey, 2008, p. 59). It is no surprise therefore to discover that the diffusion of CCTV surveillance in Europe has been more widespread in countries undergoing economic dislocation or liberalisation, such as Hungary and the UK, than it has been in "countries which have had relatively, stable welfarist-orientated governments such as Norway, Sweden, Germany and Austria" (Norris et al., 2004, p. 121). These findings are supported by more recent research on the global diffusion of open-street CCTV surveillance cameras in Brazil (Murakami Wood, 2012), Turkey (Bozbeyoglu, 2012) and South Africa (Minnaar, 2012) which reflect a broader shift in these countries away from socially progressive polices and welfare, towards exclusionary measures directed at marginalised populations. The degree of central funding committed by the state is another key factor in the global diffusion of new surveillance. As Wacquant (2010, p. 214) points out, while the neoliberal state "embraces laissez-faire at the top", it tends to "be fiercely interventionist, bossy, and pricey" when introducing new measures to control problem populations. Thus, between 1992 and 2002 the UK central government, through its City Challenge Competition and Crime Reduction Programmes, committed over a quarter of a Billion pounds of predominantly public money to the expansion of CCTV surveillance cameras (Norris et al., 2004, p. 112). As Doyle, Lippert and Lyon (2012, p. 6) point out, "the absence of similar driving initiatives by national governments is one factor explaining the much slower dissemination of public open-street camera surveillance in other" countries[6].

4. The Politics of Surveillance in the UK: Managing Problem Populations

As indicated above, the legitimating factors behind the growth of new surveillance technologies include technological potential, the rise of the personal-information economy, risk management, national security, public perceptions, new laws and neoliberalism (Bennett, Haggerty, Lyon, & Steeves, 2014, pp. 10-13). In their outline of the key drivers behind surveillance, Bennett et al. (2014, p. 11) define neo-liberalism as a set of "governmental policies that stress free trade and deregulated markets". However, as Wacquant (2009a, 2010) points out, neo-liberal policies include not only a preference for market rule, but also "an expansive and proactive penal apparatus", "welfare state devolution and retraction", and "the cultural trope of individual responsibility" (Wacquant, 2010, p. 197). While Wacquant used this framework to examine penal transformation in the USA, this broader sociological conception of "neo-liberalism" provides a useful conceptual framework for theorizing the emergence of new surveillance technologies in the UK crime control field. As we shall show below, the emergence of an expansive penal apparatus, welfare state retraction, and neo-liberal responsibilisation strategies are all central

types of exclusionary messages they send to the collectivity".

[6] As Smith (2015) points out, the neoliberal concern with economic rationalism could eventually lead to a shift from the politics of surveillance "expansion" to a politics of "diminution" as large-scale CCTV networks become a financial burden.

drivers behind the emergence of new surveillance technologies in the crime control field.

Any theory of contemporary penal change must begin by considering the wider transformation of the "field of power" ushered in by the demise of the Keynesian Welfare State (KWS) and the emergence of neo-liberalism. As a number of writers have argued, this transformation has resulted in the deautonomization of the crime control field whereby the cultural capital of criminological and legal experts has become de-valued or de-legitimated, while political capital (in relation to crime control) has become valorised[7]. As Haggerty (2004) points out, while criminal justice policy (in the USA and UK) has always been driven by political considerations, the last two decades have seen the emergence of a more explicitly symbolic politics which values political expediency above criminological research and the emergence of a technological field of expertise which has served to "displace the policy relevance of criminology" (2004, p. 222). Following the IRA bombings in the City of London in 1993, for example, a network of CCTV surveillance cameras was rapidly introduced to record traffic movement in and out of the city centre. Similar developments were reported after the attacks on September 11 in the United States when the "rush to surveillance" intensified further largely driven by developments in the political and journalistic fields (Ball & Webster, 2003). In this context, the introduction of new legislation or new surveillance technologies such as CCTV cameras is often announced at a political party conference or in the "journalistic field" before any systematic evaluation of their efficacy (see Norris, 2012, p. 254).

As Garland (2001) points out, the developments outlined above are also related to the demise of penal modernism which has witnessed the emergence of punitive law enforcement policies alongside risk-based strategies of social control. For Garland (2001, pp. 105-106), these developments are the result of "a new criminological *predicament…the normality of high crime rates* and *the acknowledged limitations of the criminal justice state*". The response to this predicament in the "crime control field" has resulted in a series of policies that are highly contradictory. Garland notes that on the one hand the state appears to be attempting to reclaim the power of sovereign command by the use of phrases like "zero tolerance", "prison works", and "three strikes". However, at the same time there has been an attempt to face up to the predicament and develop new pragmatic "adaptive" strategies including the "commercialization of justice" and a redistribution of the responsibility for crime control (2001, p. 113). While Garland (2001) sees these developments as a schizoid and disjointed response from the state to a new "criminological predicament", Wacquant (2009a, p. 301) argues that it is "a predictable organizational division in the labour of management of the disruptive poor". From this perspective, the rapid introduction of "new surveillance" technologies following highly mediatised crimes fits neatly with the "sovereign state" strategies of "denial" and "acting out" (Garland, 2001) that are manifest in the "political" and "journalistic" fields, while the emergence of actuarial regimes characterised by pre-emption, surveillance and intelligence-led policing chimes with the "adaptive strategies" (Garland, 2001) found in the penal sector of the "bureaucratic field".

As a number of writers have shown, the new surveillance practices and technologies that have been introduced in the UK are disproportionately directed towards those shorn of economic and cultural capital. In recent years, for example, probation policy in the UK has seen the widespread use of standardized assessment tools that are used to classify and "separate the more from the less dangerous" (Feeley & Simon, 1992, p. 452). These developments have facilitated the introduction of intensive supervision and surveillance programmes directed at "prolific" or "persistent" offenders which utilise compulsory drug testing, criminal profiling, electronic monitoring and police databases. As Norris (2007, p. 156) has shown, the construction of this expansive surveillance apparatus in the bureaucratic field is used to monitor those shorn of capital, typically "an unemployed, drug-using male, under the age of 21, who is likely to have been in local authority care, been excluded from school and have few, if any, qualifications". Similar developments can be found in the context of "bureaucratic welfare" regimes where a plethora of new surveillance technologies have been introduced to monitor the welfare poor (Gilliom, 2001; Wacquant, 2009a). Welfare claimants in the UK and USA are surrounded by a range of surveillance technologies and programmes that intimately oversee their eligibility for work, leisure patterns and family status. In the United States, for instance, it has become increasingly difficult to distinguish the welfare office from the probation office:

> Welfare offices have borrowed the stock-and-trade techniques of the correctional institution: a behaviourist philosophy of action a` la Skinner, constant close-up monitoring, strict spatial assignments and time constraints, intensive record-keeping and case management, periodic interrogation and reporting, and a rigid system of graduated sanctions for failing to perform properly (Wacquant, 2009a, p. 102).

The other central feature of neo-liberal regimes identified by Wacquant (2010) is the cultural trope of individual responsibility. In the crime control field, this in-

[7] The exception here of course is the influence of "new right" criminologists such as James Q. Wilson which chimes with neo-liberal thinking (see Haggerty, 2004).

volves an attempt by the state to devolve the responsibility for surveillance onto individuals and organisations. For instance, over the last two decades the CCTV Challenge Competitions and Crime Reduction Programmes devolved the responsibility for crime control in the UK on to local public-private partnerships. Moreover, empirical research in UK town centres has shown how these public-private CCTV systems can be co-opted for central state purposes and used to target "known criminals", "suspected drug addicts", and those "wanted" for the breach of bail conditions (Coleman, 2004; McCahill, 2002; Wakefield, 2003). More recent examples of responsibilisation include the Anti Money Laundering/Counter Terrorism Financing (AML/CFT) and e-Borders surveillance regimes (Ball et al., 2015). The former requires banks and building societies to monitor customer transactions and report any suspicious activity to the Serious Organized Crime Agency, while the latter requires airlines to collect passport data in advance of travel and transfer it to the UK Border Agency for screening against watch-lists (Ball et al., 2015, p. 21). Once again these surveillance regimes do not fall equally on all populations as customer activities and financial transactions are incorporated into information infrastructures which support the identification of criminals and terrorists (Ball et al., 2015).

5. Surveillance Practice: "Habitus" and "Field"

As Ball et al. (2015) have argued, surveillance theorists have tended to provide either society-wide analysis of the emergence of a surveillance society, or micro-sociological accounts of local dynamics and resistance. However, the nature of the connection between the two levels of analysis "has not been theorised in surveillance studies in a thoroughgoing way" (2015, p. 25). The work of Bourdieu may be instructive here as his entire approach to sociology was partly an attempt to develop a new direction in social theory that would steer a course between what he considered the excessive "voluntarism" of the philosopher Jean-Paul Sartre and the excessive "structuralism" of the anthropologist Levi-Strauss. What must be explained, according to Bourdieu, "is always choice within a structured situation that individuals do not themselves consciously structure" (in Couzens Hoy, 2005, p. 119). From this perspective, the actions and choices of individuals are shaped by "the internalization of the objective patterns of their extant social environment" (Wacquant, 2005, p. 137) and by the position they occupy in any given field. In an attempt to apply this approach to the study of penality, Joshua Page (2013) has argued that abstract theoretical accounts of penal transformation often fail to consider the intervening mechanisms that translate social-structural phenomena into penal practice. From this perspective, macro-level social transformations are always retranslated into the internal logic of "fields" and mediated by a field-specific "habitus" which refers to "an internal set of dispositions that shape perception, appreciation, and action" (Page, 2013, p. 152)[8]. Thus, while "macro-level, structural trends affect practice (what agents do and what decisions are made)…they do not do so automatically and without mediation" (2013, p. 154). Similar arguments can be made in relation to the crime control field. For instance, empirical research on "surveillance practice" in a range of settings has shown that despite the decline of the penal welfare model, those working within the "left hand" of the state have often opposed the measures introduced by the "right hand" of the state (Bourdieu, 1998, p. 2). In Australia, for example, practitioners working within "welfarist" working cultures obstructed the introduction of public-space surveillance cameras (Sutton & Wilson, 2004). Similarly, research has shown how "welfare agency staff assisted clients in bettering the surveillance system" through the use of "head nods (yes) or shakes (no) as the client responded to questions during intake interviews that were logging data into the system" (Gilliom & Monahan, 2012, p. 408). At the micro-level of probation practice, meanwhile, it has been shown that the "Right hand" of the state is not always aware of what the "Left hand" is doing as "risk-based" discourses are filtered through the occupational concerns of front-line practitioners who continue to be guided by the old "welfare" mentality rather than the "risk" mentality (Kemshall & Maguire, 2001).

As the neo-liberal state attempts to devolve the responsibility for crime control, new surveillance agents have entered the crime control field bringing with them a "habitus" that shapes the way new surveillance technologies are applied in practice. For instance, empirical research on the use of CCTV surveillance cameras in a shopping mall in Riyadh found that surveillance monitoring was filtered through the religious norms and social mores of those operating the systems. In this context, private security officers who recently left their tribal village used cameras not to target groups of "flawed consumers", but to target "singles", groups of males suspected of engaging in "courtship" behaviour in a sex-segregated society (Al-hadar & McCahill, 2011). In the UK, ethnographic research on the operation of CCTV systems on mass private property has shown how some corporate actors continue to work with the old "welfare" mentality, empathising with the plight of local working class youths (McCahill, 2002). One study on the use of CCTV surveillance cameras in a shopping mall situated on a deprived council estate in the north of England, reported how low paid, low status, working class security officers refused to pass on the names of "wanted" persons identified on camera

[8] The difference between "habitus" and "field" was characterised by Bourdieu "as the difference between the feel for the game and the game itself" (Couzens Hoy, 2005, p. 110).

to the local beat officer (McCahill, 2002). More recently, ethnographic observations of encounters between "flawed consumers" and private security officers in an English shopping mall revealed that despite receiving "life-time" banning orders, marginalized groups utilised social capital (i.e. collusion with private security officers) to gain access to public services that were provided on private property (McCahill & Finn, 2014). Thus, while the crime control field may have changed dramatically in recent years "neither the 'culture of control' nor the 'new penology' have fully taken root in the heads and habitus of penal agents" (Page, 2013, p. 158), or in the heads of "private" actors who often find themselves monitoring their own locales and workplace situations (McCahill, 2002)[9].

6. Surveillance, Capital and Resistance

One of Bourdieu's central contributions to social theory was to demonstrate that it is not only "economic capital" (i.e. money or property) that functions as a determinant of social position, but also "social capital" in the form of networks and social relationships, "cultural capital" such as education, skills and cultural knowledge, and "symbolic capital" which designates the authority, knowledge, prestige, or reputation that an individual or group has accumulated (Bourdieu, 1986). While previous research has shown how these forms of capital can be mobilised by the institutional actors conducting surveillance (Dupont, 2004, p. 244), this section draws upon ethnographic research to show how the subjective experience and response to surveillance is also shaped by the distribution of capitals (see McCahill & Finn, 2014). For instance, our research has shown that relatively privileged groups, such as "middle class" protesters or police officers, utilised economic, social and cultural capital to evade or contest surveillance in various ways. Protesters utilised social capital (e.g. personal contacts with senior police officers, lawyers, MPs, local councillors, journalists, and associates working in the "privacy" movement) and cultural capital (e.g. knowledge of the law) to challenge surveillance through the courts, or to discover the "fate of their data" through Freedom of Information requests. Similarly, police officers and security officers working under the gaze of CCTV surveillance cameras utilised social and cultural capital to manage not just *when* they appeared on CCTV, but also *how* they appeared on camera. In this case, knowledge of either operating the systems or visiting control rooms, enabled plural police actors to avoid the gaze of surveillance camera operators by locating themselves in "blind spots" when patrolling the shopping malls or streets. Alternatively, plural police actors would visit surveillance camera control rooms to review footage, reflect on their bodily comportment, and modify their behaviour in future "face-to-face" interactions (McCahill & Finn, 2014).

However, it is not only relatively privileged groups who utilise capitals to contest surveillance in various ways. As Bennett et al. (2010, p. 29) have suggested, "rather than assume an essential unity to cultural capital", it may be useful to explore how other forms of cultural know-how may serve to function "as sources of cultural privilege" in a range of new settings and situations. For instance, in his later work Bourdieu (2005) used the concept of "technical capital" "to refer to the distinctive assets that members of the working classes acquire through their vocational skills and pass on to their children through domestic training" (in Bennett et al., 2010, p. 29). Bourdieu (1990) also referred to the "lucidity of the excluded" to illustrate how the exclusion of marginalised groups from certain realms of privilege can often accord them a certain critical insight into the structures that oppress them (see McNay, 2000). Thus, alongside the "master" concepts of capital identified by Bourdieu, we have introduced the term *surveillance capital* to explain how surveillance subjects utilise the everyday forms of tacit knowledge that is acquired through first-hand experience of power relations to challenge the very same power relations. For instance, our ethnographic research showed how "prolific" offenders were aware that probation officers shared information with other agencies because of what they had read on the induction forms that they were required to sign. Others were aware that any information they might give away during interviews was likely to be stored on the database. One prolific offender summed it up when he said:

> Like the police that work with me make out that they're not the police and they work with probation and that, but they're full on undercover coppers. The quicker you get to learn that the better innit? You don't want to be an idiot and pretend that they're not proper police (in McCahill & Finn, 2014).

Moreover, while the information stored on databases can be treated as the source of "truth" that overrides personal testimonies, some "prolific" offenders used the existence of the "file" or "database" to avoid "opening up" and answering questions during face-to-face interviews by telling drugs workers in the probation office to "go check the file". "Prolific" offenders also used the existence of "new technologies" to evade monitoring by keeping text messages sent by the probation staff to prove that they had not missed or were

[9] Research on the Anti Money Laundering/Counter Terrorism Financing (AML/CFT) and e-Borders regime has shown how national security surveillance regimes were filtered through the "habitus" of corporate actors who used e-Borders to explore commercial opportunities arising from the extra customer contact (Ball et al., 2015).

not late for appointments. One "prolific" offender used the data that had been extracted from his body to his advantage when he requested photo-copies of any "negative" drug tests to take home and show his partner that he was not using drugs. Family members of "prolific" offenders also used *surveillance against surveillance* to support their case when confronted by the police. One mother kept fragments of her son's "digital persona" (electronically-recorded consumer transactions) to challenge police decisions to question or arrest her son. While *surveillance capital* may not be easily translated into other forms of "capital", it does provide surveillance subjects with a degree of agency in local and specific settings.

As Bourdieu argued, while "those who dominate in a given field are in a position to make it function to their advantage…they must always contend with the resistance, the claims, the contention…of the dominated" (Bourdieu & Wacquant, 1992, p. 102). However, the French author was also well aware of the ironies of resistance and the potential for these strategies to reproduce existing social divisions. In an attempt to conceptualize these issues, he used "the term 'regulated liberties' to denote a more complex relation between the dominant and its subjects" (Bourdieu, 1990, p. 102). Here Bourdieu (1990) drew attention to what he described as "the unresolvable contradiction of resistance", whereby the dominated "can resist by trying to efface the signs of difference that have led to their domination", or they can "dominate their own domination by accepting and accentuating the characteristics that mark them as dominated" (in Couzens Hoy, 2005, p. 135). In recent years, a number of writers have drawn upon these ideas to explore the relationship between surveillance, body capital and class divisions following the shift from an industrial society organised around manufacturing and heavy industry to a post-industrial society dominated by the service sector and consumerism. In the field of employment the decline of heavy industry which valued a "type of 'body capital' forged through notions of physical hardness and a patriarchal breadwinner", now seems out of step in a consumer or service economy "that values flexibility, keyboard proficiency, telephone communication skills and personal presentation" (Nayak, 2006, p. 817). The exclusion of working class males from the field of employment in post-industrial cities is compounded by exclusion from public spaces due to embodied attributes which are considered "out of place" in the new spaces of consumption. Nayak (2006, p. 821) for example has shown how the "body capital" of young working males in Newcastle led to their exclusion from clubs and bars in the city centre. He refers to how so-called "charvers" "hold their head" and "arch their backs when walking". The targeting practices of open-street CCTV operators in UK cities are also said to fall disproportionately on those who look "too confident for their own good" or who had their "head up, back straight, upper body moving too much", or those who were "swaggering, looking hard" (Norris & Armstrong, 1999, p. 122). In our ethnographic account of the subjective experience of surveillance in a northern city in the UK, we showed how marginalised groups responded to CCTV monitoring by covering their faces with hats and scarves, flicking "V signs" at surveillance camera operators, and throwing bricks at cameras. Of course, those who obscure their faces with clothing or who oriented their behaviour to camera operators through confrontation and abusive gestures are often singled out for further attention by surveillance camera operators (see Norris, 2003, p. 265). In this context, the body becomes both a "performance" *and* a "straitjacket" (Shilling, 2003) as the "bodily hexis" (dialect, accent, dress, body posture and demeanour) conveys resistant impressions that potentially leads to further surveillance and exclusion (McCahill & Finn, 2014).

7. Conclusion

The surveillance studies literature has been dominated by Foucaultian and Deleuzian-inspired perspectives on "discipline" (Foucault, 1977) and "control" (Deleuze, 1992). The aim of this paper has not been to "go beyond" Foucault or Deleuze. The work produced by these towering intellectuals is far too important for that and will no doubt continue to frame theoretical debates on surveillance for decades to come. Instead, our aims were much more modest and were simply to propose an alternative approach to the study of surveillance that replaced a discursive analysis of historical texts with empirically-informed "field" theory. As Haggerty (2006, pp. 41-42) argues, while surveillance theorists might want to embrace many of Foucault's insights, they may also want to reserve "space for modestly realist projects that analyze the politics of surveillance or the experiences of the subjects of surveillance". To do this, we argued, required a different approach to Foucault whose main concern was with the forms that power relations take and "the techniques they depend upon, rather than upon the groups and individuals who dominate or are dominated as a consequence" (Luke, 2005, p. 89). As Foucault (2001, p. 331) explained, "the main objective of…struggles is to attack not so much such-or-such institution of power, or group, or elite, or class but, rather, a technique, a form of power". Thus, whereas Foucault begins with an "'*ascending* analysis of power starting from its infinitesimal mechanisms', Bourdieu gives priority to a focused analysis of the nexus of institutions that ensures the reproduction of economic and cultural capital" in the wider field of power (Wacquant, 2005, p. 145).

Drawing upon this approach, we argued that the demise of the Keynesian Welfare State (KWS) and the rise of neo-liberal economic policies in the UK has placed new surveillance technologies at the centre of a reconfigured "crime control field" (Garland, 2001) designed to control the problem populations created by neo-liberal economic policies (Wacquant, 2009a). At the same time, however, we suggested that field theory offers the potential to examine national variations in the up-take of new surveillance technologies by showing how globalizing forces and wider social changes are filtered through the political and juridical fields of different national jurisdictions. This approach also provides a bridge between society-wide analysis and micro-sociology by showing how surveillance practice is filtered through the existing organisational, occupational and individual concerns of surveillance agents. Following this, we situated the introduction of new surveillance within "fields of struggle", arguing that the distribution of various forms of "capital"—economic, social, cultural and symbolic—operate as a range of goods or resources that structure the dynamics of surveillance practices and power relations in the crime control field. In this respect, our analysis involved a critical engagement with two theoretical traditions−Focaultian approaches which provide dystopian visions of the power of state surveillance while underplaying agency, and interactionist perspectives on the "everyday politics of resistance" (Marx, 2002; J. C. Scott, 1990) which often fail to consider how "the interaction itself owes its form to the objective structures which have produced the dispositions of the interacting agents and which allot them their relative positions in the interaction and elsewhere" (Bourdieu, 1977, p. 81).

To sum up therefore we have attempted to combine a macro-level analysis which explores how globalizing forces are filtered through the "field of power" in different national jurisdictions, with a micro-level analysis which shows how new surveillance measures are mediated by the "habitus" of surveillance agents and surveillance subjects. This approach, we argue, advances our understanding of surveillance politics in two ways. First, it can "act as solvent of the new neoliberal common sense that 'naturalizes' the current state of affairs" (Wacquant, 2009b, p. 129) by demonstrating that there are alternatives to the "bad example" set by neo-liberal countries such as the UK where the "processes of normalisation of surveillance have gone much further than elsewhere" (Murakami Wood & Webster, 2009, p. 260). Second, it provides a corrective to "top-down" surveillance theories which continue to portray surveillance subjects as "docile bodies", rather than social actors who can contest power relations in a field that is very much skewed against them.

Acknowledgments

The author would like to thank three anonymous reviewers and the editors of this special edition for their insightful comments and advice. Special thanks also to Simon Green and Mark Johnson for reading and commenting on an earlier draft of this paper. This paper grew out of an Economic and Social Research (ESRC)-funded project, Grant RES-062-23-0969. For an overview of research data and other information see: http://www.esrc.ac.uk/my-esrc/grants/RES-062-23-0969/read

Conflict of Interests

The author declares no conflict of interests.

References

Alhadar, I., & McCahill, M. (2011). The use of surveillance cameras in a Riyadh shopping mall. *Theoretical Criminology*, *15*(3), 315-330.

Ball, K., & Webster, W. (2003). The intensification of surveillance. In K. Ball & F. Webster (Eds.), *The intensification of surveillance: Crime, terrorism and warfare in the information age*. (pp. 1-15). London: Pluto Press

Ball, K., Canhoto, A., Daniel, E., Dibb, S., Meadows, M., & Spiller, K. (2015). *The private security State*. Frederiksberg: CBS Press.

Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (2014). *Transparent lives: Surveillance in Canada*. Athabasca University: Athabasca University Press.

Bennett, T., Savage, M., Silva, E., Warde, A., Gayo-Cal, M., & Wright, D. (2010). *Culture, class, distinction*. London: Routledge.

Benson, R. (2005). Mapping field variation: Journalism in France and the United States. In R. Benson & E. Neveu (Eds.), *Bourdieu and the journalistic field* (pp. 85-112). Cambridge: Polity Press.

Bigo, D. (2000). Liaison officers in Europe: New officers in the European security field. In J. W. E. Sheptycki (Ed.), *Issues in transnational policing* (pp. 67-99). London: Routledge.

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives*, *27*(1), 63-92.

Bogard, W. (2006). Surveillance assemblages and lines of flight. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 97-122). Cullompton: Willan.

Bogard, W. (2012). Simulation and post-panopticism. In K. Ball, K. Haggertyand, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 3-37). Abingdon: Routledge.

Bourdieu, P. (1977). *Outline of a theory of practice*. Cambridge: Cambridge University Press.

Bourdieu, P. (1984). Rethinking the State: Genesis and structure of the bureaucratic field. *Sociological Theory*, *12*(1), 1-18.

Bourdieu, P. (1990). *In other words: Essays towards a re-*

flexive sociology. Cambridge: Polity Press.

Bourdieu, P. (1991). *Language and symbolic power*. Cambridge: Harvard University Press.

Bourdieu, P. (1998). *Acts of resistance against the new myths of our times*. Cambridge: Polity Press.

Bourdieu, P. (2005). *The social structures of the economy*. Cambridge: Polity Press.

Bourdieu, P., & Wacquant, L. (1992). *An invitation to reflexive sociology*. Chicago: University of Chicago Press.

Bozbeyoglu, A. C. (2012). The electronic eye of the police: The provincial information and security system in Istanbul. In A. Doyle, R. Lippert, & D. Lyon (Eds.), *Eyes everywhere: The global growth of camera surveillance* (pp. 139-155). London: Routledge.

Cavadino, M., & Dignan, J. (2006). *Penal systems: a comparative approach*. London: Sage.

Coleman, R. (2004). *Reclaiming the streets: Surveillance, social control and the city*. Cullompton: Willan.

Couzens Hoy, D. (2005). *Critical resistance: From post-structuralism to post-critique*. Massachusetts: MIT Press.

Dandeker, C. (1990). *Surveillance, power and modernity: Bureaucracy and discipline from 1700 to the present day*. Cambridge: Polity Press.

Deleuze, G. (1992). Postscript on the societies of control. *October*, *59*, 3-7.

Doyle, A., Lippert, R., & Lyon, D. (2012). Introduction. In A. Doyle, R. Lippert, & D. Lyon (Eds.) *Eyes everywhere: The global growth of camera surveillance* (pp. 1-19). London: Routledge.

Dupont, B. (2004). Security in the age of networks. *Policing and Society*, *14*(1), 76-91.

Feeley, M., & Simon, J. (1992). The new penology. *Criminology*, *30*(4), 449-474.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. London: Allen Lane.

Foucault, M. (2001). Interview with Michel Foucault. In J. D. Faubion (Ed.), *Essential works of Foucault 1954–1984, Volume 3; Power*. London: Penguin Books.

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford: OUP.

Giddens, A. (1985). *The nation state and violence: Volume two of a contemporary critique of historical materialism*. Cambridge: Polity Press.

Gilliom, J. (2001). *Overseers of the poor: Surveillance and the limits of privacy*. Chicago: University of Chicago Press.

Gilliom, J., & Monahan, T. (2012). Everyday Resistance. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 405-11). Abingdon: Routledge.

Haggerty, K. D. (2004). Displaced expertise: Three constraints on the policy-relevance of criminological thought. *Theoretical Criminology*, *8*(2), 211-231.

Haggerty, K. D. (2006). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 23-45). Cullompton: Willan.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622.

Haggerty, K. D., & Ericson, R. V. (2006). The new politics of surveillance and visibility. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 3-25). Toronto: University of Toronto Press.

Johnston, L., & Shearing, C. (2003). *Governing security: Explorations in policing and justice.* London: Routledge.

Kemshall, H., & Maguire, M. (2001). Public protection, partnership and risk penality: The multi-agency risk management of sexual and violent offenders. *Punishment and Society, 3*(2), 237-264.

Lacey, N. (2008). *The prisoners' dilemma: political economy and punishment in contemporary democracies*. Cambridge: Cambridge University Press.

Loveman, M. (2005). The modern State and the primitive accumulation of symbolic power. *American Journal of Sociology*, *110*(6), 1651-1683.

Luke, S. (2005). *Power: A radical view*. Basingstoke: Palgrave Macmillan.

Lyon, D. (1993). An electronic panopticon? A sociological critique of surveillance theory. *The Sociological Review*, *41*(4), 653-678.

Lyon, D. (1994). *The electronic eye: The rise of the surveillance society*. Cambridge: Polity Press.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University.

Marx, G. T. (2002). What's new about the new surveillance? Classifying for change and continuity. *Surveillance and Society*, *1*(1), 9-29.

Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues*, *59*(2), 369-390.

McCahill, M. (2002). *The surveillance web: The rise of visual surveillance in an English city*. Devon: Willan

McCahill, M., & Finn, R. L. (2014). *Surveillance, capital and resistance: Theorizing the surveillance subject*. Abingdon: Routledge.

McNay, L. (2000). *Gender and agency: Reconfiguring the subject in feminist and social theory*. Cambridge: Polity.

Minnaar, A. (2012). The growth and further proliferation of camera surveillance in South Africa. In A. Doyle, R. Lippert, & D. Lyon (Eds.), *Eyes everywhere: The global growth of camera surveillance* (pp. 100-121). London: Routledge.

Murakami Wood, D. (2009). The surveillance society: Questions of history, place and culture. *European Journal of Criminology*, *6*(2), 179-194.

Murakami Wood, D. (2012). Cameras in context: A comparison of the place of video surveillance in Japan and Brazil. In A. Doyle, R. Lippert, & D. Lyon (Eds.), *Eyes everywhere: The global growth of camera surveillance* (pp. 83-99). London: Routledge.

Murakami Wood, D., & Webster, W. (2009). Living in surveillance societies: The normalisation of surveillance in Europe. *Journal of Contemporary European Research*, 5(2), 259-273.

Nayak, A. (2006). Displaced masculinities: chavs, youth and class in the post-industrial city. *Sociology*, 40(5), 813-831.

Nelken, D. (2005). When is a society non-punitive? The Italian case. In J. Pratt, M. Brown, S. Hallsworth, & W. Morrison (Eds.), *The new punitiveness: Trends, theories, perspectives* (pp. 218-238). Cullompton: Willan.

Norris, C. (2003). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 249-281). New York: Routledge.

Norris, C. (2007). The intensification and bifurcation of surveillance in British criminal justice policy. *European Journal on Criminal Policy and Research*, *13*(1−2), 139-158.

Norris, C. (2012). The success of failure: Accounting for the global growth of CCTV. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 251-58). Abingdon: Routledge.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society*. Oxford: Berg.

Norris, C., McCahill, M., & Murakami Wood, D. (2004). The growth of CCTV: A global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance and Society*, *2*(2−3), 110-135. Retrieved from www.surveillance-andsociety.org

Page, J. (2013). Punishment and the penal field. In J. Simon & R. Sparks (Eds.), *The Sage handbook of punishment and society* (pp. 152-166). London: Sage.

Scott, A. (2013). We are the State: Pierre Bourdieu on the State and the Political Field. *Rivista di Storia Idee*, *2*(1), 56-70. Retrieved from http://www.academia.edu/4296007/We_are_the_state._Pierre_Bourdieu_on_the_state_and_political_field

Scott, J. C. (1990). *Domination and the arts of resistance: Hidden transcripts*. New Haven: Yale University Press.

Shilling, C. (2003). *The body and social theory*. London: Sage.

Simon, J. (2007). *Governing through crime*. Oxford: OUP.

Smith, G. J. D. (2015). *Opening the black box: The work of watching*. London: Routledge.

Staples, W. G., & Decker, S. K. (2008). Technologies of the body, technologies of the self: House arrest as neo-liberal governance. In M. Deflem (Ed.), *Surveillance and governance: Crime control and beyond* (pp. 131-149). Bingley: Emerald Group Publishing Limited.

Sutton, A., & Wilson, D. (2004). Open-street CCTV in Australia: The politics of resistance and expansion. *Surveillance and Society*, *2*(2−3), 310-322.

Swartz, D. L. (2004). *The State as the central bank of symbolic credit*. Paper presented at the American Sociological Association 99th Annual Meeting, August 14−17, 2004, San Francisco, USA. Retrieved from http://people.bu.edu/dswartz/articles/10.html

Thompson, J. B. (1991). Editors introduction. In P. Bourdieu (Ed.), *Language and symbolic power* (pp. 1-31). Cambridge: Polity Press.

Wacquant, L. (1993). From ruling class to field of power: An interview with Pierre Bourdieu. *La Noblesse d'Etat*, *Theory, Culture and Society*, *10*(3), 19-44.

Wacquant, L. (2005). Symbolic power in the rule of the state nobility. In W. Wacquant (Ed.), *Bourdieu and democratic politics*. Cambridge: Polity Press.

Wacquant, L. (2009a). *Punishing the poor: The neoliberal government of social insecurity*. Durham and London: Duke University Press.

Wacquant, L. (2009b). The body, the ghetto and the penal State. *Qualitative Sociology*, *32*(1), 101-129.

Wacquant, L. (2010). Crafting the neoliberal State: Workfare, prisonfare, and social insecurity. *Sociological Forum*, *25*(2), 197-220.

Wakefield, A. (2003). *Selling security: The private policing of public space.* Cullompton: Willan.

About the Author

Dr. Michael McCahill

Michael McCahill's research focuses on the social impact of "new surveillance" technologies in the context of policing and criminal justice. His books include *The Surveillance Web* (2002) (winner of the British Society of Criminology book prize 2003), *Surveillance and Crime* (2011) (with Roy Coleman), and *Surveillance, Capital and Resistance* (with Rachel L. Finn).

COGITATIO

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 21-41
Doi: 10.17645/mac.v3i2.220

Article

Surveillance and Resilience in Theory and Practice

Charles D. Raab [1,]*, Richard Jones [2] and Ivan Szekely [3]

[1] School of Social and Political Science, University of Edinburgh, Edinburgh, EH8 9LD, UK; E-Mail: c.d.raab@ed.ac.uk
[2] School of Law, University of Edinburgh, Edinburgh, EH8 9YL, UK; E-Mail: richard.jones@ed.ac.uk
[3] Eotvos Karoly Policy Institute, 1088 Budapest, Hungary; E-Mail: szekelyi@ceu.edu

* Corresponding author

Submitted: 6 January 2015 | In Revised Form: 28 April 2015 | Accepted: 5 May 2015 |
Published: 30 September 2015

Abstract
Surveillance is often used as a tool in resilience strategies towards the threat posed by terrorist attacks and other serious crime. “Resilience” is a contested term with varying and ambiguous meaning in governmental, business and social discourses, and it is not clear how it relates to other terms that characterise processes or states of being. Resilience is often assumed to have positive connotations, but critics view it with great suspicion, regarding it as a neo-liberal governmental strategy. However, we argue that surveillance, introduced in the name of greater security, may itself erode social freedoms and public goods such as privacy, paradoxically requiring societal resilience, whether precautionary or in mitigation of the harms it causes to the public goods of free societies. This article develops new models and extends existing ones to describe resilience processes unfolding over time and in anticipation of, or in reaction to, adversities of different kinds and severity, and explores resilience both on the plane of abstract analysis and in the context of societal responses to mass surveillance. The article thus focuses upon surveillance as a special field for conceptual analysis and modelling of situations, and for evaluating contemporary developments in “surveillance societies”.

Keywords
democracy; privacy; public goods; resilience; security; surveillance

Issue
This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction

The dramatic revelations made in 2013 by Edward Snowden concerned the extensive and intensive surveillance operations of USA and allied intelligence services, involving covert collection of communications data on a massive scale, with or without clear legal warrant and often with the complicity of private communications, computing and media companies (Greenwald, 2014). Many of the specific and previously top-secret mass surveillance programmes that Snowden revealed were shown to be operating on an unimaginably huge scale. Increasing public knowledge of these practices has stimulated a variety of responses from citizens, governments, civil society organisations, and other interests. Their views include a search for types of response that include opposition, a plea for regulation and control, and better ways of shaping the relationship between national security and the requirements of liberal democracy. Reactions by privacy and Internet activists and advocates, by some parts of the media, and by a few politicians and lawyers, have been among the most considered, forceful and promising, with proposed reforming measures ranging from the technical to the legal, regulatory and political. However, we do not yet possess the conceptual apparatus to model the relationship these disparate means of addressing surveillance have to one another, nor to their collective efficacy in the face of the threats posed by mass surveillance programmes.[1]

Although mass surveillance started well before 9/11, its rapid expansion since then is often understood as a reaction to the terrorist attacks. Indeed, many countries have expanded their counter-terror activities over the same time period, and the term "resilience" is often found in official discourses of counter-terror strategies, as well as serving as an analytical term in security studies and other policy areas. It also features in popular but vague inspirational language that is meant to connote an attitude, or stance, to be taken in a wide variety of adverse circumstances. The use of this term (along with the related term, "resilient") has noticeably proliferated in recent years, applied to a vast array of systems, contexts, processes and policies. White and O'Hare (2014), for example, found that some 800 official UK policy documents published since 2005 contained versions of the term, including in the area of counter-terrorism. The properties of resilience are considered by policy-makers generally to be beneficial, and the aim of making human and natural systems resilient taken to be worthy of approval as well as deserving of the allocation of resources. Evaluations of individual, group, societal and system performance in terms of their resilience have become commonplace, and criticism of non-resilience has become justified in the name of improvement. Few would wish to be labelled with various possible antonyms: brittle, fragile, inflexible, unbending. In sum, the art, craft and science of making people and things resilient all flourish in the face of threats that may or may not be known or predicted.

Amidst this proliferation, framing theory and policy in terms of "resilience" has attracted its critics as well as engendered debate. Chandler established the journal *Resilience* "to critically engage with the world around us, to ask new questions of it" (Chandler, 2013a). The study of resilience is seen as multidimensional, ambitiously embracing practices, policies, discourses, processes, spaces of construction, economics, politics, and subjectivities. The concept "resilience" is used almost magnetically to re-orientate the particles of diverse fields, disciplines, approaches and substantive research around a new way to frame and comprehend their complementarity. Against this initiative, Neocleous has attacked "resilience" as a project for "colonizing the imagination" and making the state and capitalism more resilient. It represents an uncritical diversion from the need for resistance that follows the agenda of neoliberalism (Neocleous, 2013a, p. 7; see Chandler, 2013b; Neocleous, 2013b). Recent debate over the usefulness or, conversely, the danger, of adopting a "resilience" approach has taken place in the context of international relations discourse, and specifically with reference to liberal intervention to solve a range of local and global problems (Chandler, 2015). Yet Bourbeau, who notes the proliferation of "resilience" analysis in many fields, observes that in the literature on world politics, security and "securitisation", "there is very little coherence and consensus as to the nature and substance of resilience. The term is employed but rarely unpacked, let alone theoretically analysed" (Bourbeau, 2013, p. 3).

Although the present article is situated broadly within the study of security, we do not aim to enter the current debate on the plane inhabited by its protagonists. Whilst borrowing conceptual elements from some of those engaged in the latter, we aim—in Bourbeau's terms—to analyse "resilience" theoretically in order to use it in the context of *surveillance*, which we believe is a novel application. This is done in order to contribute to understanding the effects of surveillance. Although surveillance practiced in aid of (national) security or public safety is indeed a threat to desired and desirable personal and social values, we are also sceptical about easy assumptions about the reality of a "slippery slope" that demands only resistance.

We thus explore societal resilience to the threats to democracies posed by the current mass surveillance of communications and other applications of surveillance technologies and practices. This exploration is done through modelling resilience to surveillance, which also embraces "sleepwalking" into a surveillance society and "waking up". Surveillance *itself* is a resilience tool wielded in government policy, used instrumentally—and discursively justified—to increase collective, individual, or infrastructural security against certain threats, such as terrorism or breakdowns of public order. However, despite the supposed benefits of surveillance as part of a resilience strategy in the face of threats, surveillance's prevalence, intensity, and use of specialised resources including access to personally identifiable information may actually erode privacy along with a host of other "public goods": associated rights, freedoms, ethical principles, security, and other values that it is designed to protect, including democracy itself (Raab, 2012; Raab, 2014). In this erosion, surveillance may exemplify the "dark side" of resilience (Bourbeau, 2013, p. 4).

These prospects of threat and response are examined through the novel visual presentation of possible alternative trajectories. The innovation of this portrayal rests, however, on the fairly well-established conception—that we share with others (see Bourbeau, 2013, p. 7)—of resilience as *process* and not only as a label for a set of *qualities* or properties of an individual,

[1] This article emerges from the IRISS (Increasing Resilience in Surveillance Societies) Project (EC Grant Agreement No. 290492), in which the authors were partners, and which conceived the notion of employing resilience strategies against surveillance systems (see http://irissproject.eu/). In this article, we develop further an analysis of resilience to surveillance.

group, or society deemed to be "resilient". The theoretical possibilities outlined by these trajectories embrace all the engineering, ecological, and socio-ecological subtypes of resilience sketched by Bourbeau (2013, p. 9, Table 1), and as such, rather than rely on a singular *definition* of resilience, we present resilience as an overarching term within which the different subtypes may come into play. Turning the tables on the construction of surveillance as resilience to a conventional array of threats to security and safety, the article also further develops the argument that the practices and policies of resilience can be used *against* surveillance itself, exploring how societies may remain democratic in the face of what some writers have described as the deeply negative impacts that surveillance practices otherwise might have (e.g., Lyon, 2003a, 2003b; Čas et al., 2015; Raab et al., 2015; see also Wright & Kreissl, 2015).

Whilst privacy is the value, right, or public good most frequently said to be implicated in the employment of surveillance for national security or public safety, we do not assume that "privacy" has a singular, easily grasped, consensual meaning. It is commonplace in the literature on privacy to construe it as a cluster or "family" of values (e.g., Solove, 2008) that are prized for a variety of instrumental or intrinsic reasons, and that may be differently implicated in different norm-related contexts (Nissenbaum, 2010). There are several discernable types of privacy, each associated with one or more relatively distinctive principles, rights or freedoms, including dignity, autonomy, freedom of expression, and several others that form part of the familiar canon of individual rights and public goods inherent in liberal democracy (Wright & Raab, 2014). Our analysis of what is at stake in the deployment of surveillance embraces, in general terms, any or all of these. There is no space presently to disaggregate this understanding and to discuss each among the variety of public goods; we highlight the consequences of surveillance for privacy and security because these are the values that are most prominent in current discourse and policy.

The central arguments of this article are that the concept of resilience can usefully be applied to the study of surveillance; that resilience cannot be assumed to happen, and may in fact fail; that several different outcomes are indeed possible; that the diagrammatic approach we demonstrate usefully offers a way of incorporating different subtypes of resilience (e.g., "bouncing back") within a unified umbrella framework; and that our diagrammatic approach facilitates the representation and modelling of different scenarios and outcomes. The article's argument develops in three steps: it (1) refers to some existing models of resilience and abstracts them from their specific previous contexts before (2) developing a more varied and general model of resilience. It then (3) applies this specifically to the topic of surveillance.

2. Resilience: Some Examples in Discourse and Practice

The concept of "resilience" is identified in all kinds of natural and social phenomena where threats to integrity and identity are faced by physical objects, social goods and ethical values, or social relationships. Persistence and change are the resultant and alternative states of a host of small or large measures taken in response to, or in anticipation of, the challenges that are posed, although whether something is deemed to have persisted or changed—and how much—is not necessarily objectively determined: it is often a matter of subjective perception and conventional agreement or disagreement. This is a generic problem in the analysis of system change or persistence, and is inherent in, for example, the understanding, within policy studies, of incremental (or intra-structural) and large (or fundamental and structural) change (Braybrooke & Lindblom, 1963, p. 62 and Chapter 4).

Nevertheless, while "resilience" is held to be a widely-applicable concept, its meaning as well as the practical measures it indicates are disparate. The latter point in different ways to the means of protecting, detecting, and responding to the consequences of threats, attacks, disasters and other adverse events. We do not attempt to define the term precisely, although some of its most important connotations are germane to our further analysis and are conveyed in section 4. Some examples of resilience, threat or attack in different contexts and domains can be found in official documents, and are briefly indicated here. Documentary materials drawn from UK government departments include emergency planning (UK Cabinet Office, 2013), cyber security (UK Cabinet Office, 2011a), community resilience (UK Cabinet Office, 2011b), and counter-terrorism strategy (UK Home Office, 2011). Some UN documents concern global sustainability and development (United Nations Secretary-General's High-level Panel on Global Sustainability, 2012), disaster risk reduction (UN System Task Team on the Post-2015 UN Development Agenda, 2012), pandemics and health (Ban, 2009), human rights (Yusuf, 2012), counter-terrorism (UN Security Council, Counter-Terrorism Committee (CTED), 2013), and crime-prevention (UN Commission on Narcotic Drugs/Commission on Crime Prevention and Criminal Justice, 2010). Several points can be derived from this very selective canvass:

- "Resilience" is sometimes undefined but refers to a coherent set of objectives and implementation measures in the face of human and natural threats to vital interests such as national security, food supply and community functioning.
- The resilience strategy relies upon planned, co-ordinated efforts across organisations at different

levels, and among participants with defined roles and responsibilities.

- "Resilience" enjoys a certain *political* appeal, possibly because the term suggests strength, robustness and fortitude.
- "Resilience" is also attractive to *administrators*, perhaps because it involves skills in problem analysis, strategic planning, and policy implementation.
- The meaning of "resilience" requires interpretive skills because it is not always evident, although its connotation may be clear in terms of strategy and practical measures; however, "resilience to surveillance" is more elusive.
- Even when the term is not explicitly used, it remains possible to construct a plausible scenario that identifies the threat, what is threatened, and how the threat can be countered through preventive or remedial measures.
- Preventative and preparedness measures—not the same thing—loom large across fields where threats or adverse events vary in terms of their inevitability, and therefore in the nature and dynamics of resilience.

Most of the uses of the term are with regard to national or community security and safety in the face of natural or man-made disasters and threats in some near or far future, or with regard to strategies for economic and social development. In some examples, the use of surveillance, including monitoring or other means of information gathering and social control, is considered to be part of a resilience policy or strategy.

A further relevant observation points up a distinction between resilience as a *property* of a society, community or an individual, and resilience as the *activities* undertaken to bounce back or to anticipate some threat. For example, it is possible to distinguish between two different meanings of the term "community resilience". The first is the kind of localised planning and contingency measures often encouraged by government as a means for localities to cope with sudden adverse environmental conditions or terrorist attacks, and to work alongside "first responders". The second kind is the more intrinsic or "organic" quality of psychological or community social solidarity evident in response to certain adverse events, suggesting that far from being fractured by the adverse event, individual psyches and communal bonds are resilient to damage and may even be part of a wider community-rebuilding process (see also Hall & Lamont, 2013a).

Various theories may be found in the social sciences—for example, sociology and criminology—to account for communal "organic" resilience. For example, Durkheim (1984 [1893], pp. 53-67) famously characterises fundamental societal ties in terms of "social solidarity", comprised both of social-economic interdependence on others and of shared moral values. More recently, Putnam (2000) has sought to explain why certain places or regions display greater civic vibrancy, arguing that factors such as social networks (and voluntary associations in particular) build trust and links between local people, and Sampson (2008) has argued that the concept of "collective efficacy" can explain how mutual local support may be used to achieve particular collective goals. In each case, these theorists have sought to explain empirical differences in social cohesion, both between different places and over time, finding that such cohesion is by no means inevitable. While community resilience is often assumed to be desirable, its capabilities could be used by government as a pretext for transferring responsibility for contingency management to the local level, and could even perhaps induce communities to learn to withstand events or situations that they should not have to tolerate (see also Walklate & Mythen, 2015, Chapter 6).

We now highlight at greater length a contrasting example—the study of dictatorial and post-dictatorial regimes—that relates to an overtly "political" context rather than one concerning natural or man-made disasters or law-enforcement. Here the focus is upon how, and to what extent, societies show signs of resilience in relation to the exercise of political power and the distribution of resources. In this illustration, "resilience" becomes more easily seen as neither necessarily a "good thing" nor necessarily a "pro-security" concept. Similarly, Bourbeau (2013, pp. 7-8, 10) refers to resilience's undesirable "dark side" and its dependency on context; Marx (2015, p. 16) makes a similar argument in relation to "resistance" and to "security" in general. Seeing these regimes in transformation also brings to light concrete developments that will be exemplified on a more abstract and conceptual level later in this article.

In the Soviet era in East and Central Europe, the wide range of political regimes experienced periods of change from dictatorship through transitional phases leading towards forms of democratic system. This transformation brings into view a tension between the political regime and the society, casting light on different meanings and manifestations of "resilience": societal resilience towards the dictatorial system, and the resilience of dictatorial systems themselves towards political and societal changes and towards external international pressure. Citizens, groups and institutions developed a resilience capability towards changes at various levels.

At the individual level, for example, families from the pre-war upper middle class kept their large flats if they formally accepted expropriation and nationalisation of the flats and formally registered co-tenants who had never actually lived there. Another resilience strategy of certain educated families was to commission forged paintings of famous painters from skilful local artists, since preserving and storing artworks acknowledged as part of the cultural assets of the county, for the preserving and storing of which the state galleries had no space, made them eligible for possessing an extra room in their flats. Tolerance shown to dissident groups and their *samizdat* (clandestine) publications contributed to resilience of the system and its citizens. For citizens who accepted the regime, family life and personal economy were developed through small-scale semi-private enterprise and informal economic networks. Those in opposition in underground movements developed resilience through a variety of means. In addition, the degree of a regime's repressiveness, and its use of ubiquitous surveillance in the era of the Stasi, the Securitate and similar organisations shaped opponents' behaviour and resilience. These and other characteristics enabled the regimes to reduce national and international tensions, to adapt to changing environments, and to resist shock-like impacts.

In the period of democratic transformation, the "Velvet Revolution" (Czechoslovakia) or the "rule-of-law revolution" of 1989 (Hungary) can be seen in terms of structural resilience that retained the legal and administrative framework. There is a strong tradition of resilient personal survival through social and political influence spanning transitional regime changes. Members of the former political and economic elite retained their influence by taking over state-owned companies, and the discredited secret services soon reconsolidated themselves. Even where their leaders were replaced with trustworthy pro-democratic people, many personnel remained in office, together with their organisational culture, and adapted to the changing environment. In some countries in the post-dictatorial period (e.g., Hungary), new organisations, the enforceability of individual rights and freedoms, and the capitalist economy created a window for the establishment of new institutions and international relationships. However, it is not clear whether the resilience of all social strata has persisted and become stronger. Some new democratic political organisations proved vulnerable and short-lived. Trade unions became marginalised, and the position and living standards of the unskilled and the intellectuals declined.

Societal resilience specifically towards *surveillance* in the post-dictatorship era also deserves attention. After the changes, the fear of the regime was replaced by a fear of crime. Societies under long authoritarian rule have virtually skipped the period of democratic modernity and jumped directly into the surveillance culture of postmodernity (Los, 2002). The lack of historical experience resulted in increased vulnerability and decreased resilience towards new forms and technologies of surveillance, as individuals became more susceptible to business and marketing offers and industry-driven surveillance (Szekely, 2008). In those former dictatorial regimes where personal and family life were more resilient, and although private surveillance was not conceived as potentially harmful, suspicion against state surveillance remained high.

The lessons learnt from this non-democratic and transitional context are that:

- In the perspective of democracy, a resilient dictatorship, in which non-democratic forms of political life and the careers of privileged elites may be able to survive shocks and defeats, is clearly not "good", whereas civil-societal resistance ("resilience") to the dictatorship's surveillance strategy appears politically desirable.
- The general question, "is resilience desirable?" is therefore germane in any example.
- More generally, it is important to look at the passage of historical time in analysing the sequences of adverse events and responses in order to conceptualise resilience as a trajectory.

All the above illustrations show the diversity of resilience practices and meanings in different contexts. Our argument here is (1) that resilience has become a major theme in UK and UN government policy today, particularly in relation to security matters; (2) that there are various political dimensions to this; and (3) that whatever one's political evaluation of how resilience is operating in a given area, the twin policy themes of (a) assessing the "amount" of resilience present and (b) seeking to increase this through developing better processes seem very powerful from a policy-making perspective.

Before we focus upon the domain of *surveillance* as the set of specific events and practices towards which resilience may be oriented, we first explore the theoretical grounding of the concept of resilience and locate our own efforts within its literature.

3. Theoretical Underpinning of "Resilience"

The concept of "resilience" has certain linkages with conceptual and theoretical writing on general systems and cybernetics—based on the analysis of communication and control—that discuss natural and social processes involving changes of state or restoration over time, threats to existing states of affairs, and/or interactions between actors and the "world" they seek to change or regulate. There is only space here to draw attention to the heuristic value of such conceptual frameworks for deriving points or questions that may be useful in the analysis of resilience.

General systems theory posits the notion of a system and its environment, and analyses the relationship between parts of a system, their contribution to the whole, and the relationship of the system to its environment(s) (Demerath & Peterson, 1967; Deutsch, 1963; Easton, 1965; Emery, 1969; Parsons, 1951; Wiener, 1954). Changes can be generated internally to a system or as an effect of its environment. Central to such theory are concepts such as equilibrium, stability, homeostasis, and the normal states of systems in terms of their internal organisation or in relation to their environments. Systems theory and cybernetics are replete with themes and concepts of organisation and disorganisation, the degradation (entropy) and reinforcement of states of being, adaptation, stability and instability, order and chaos, flexibility and rigidity, communication, information and control, self-organisation and feedback, and many more. They provide a conceptual language for talking about how systems maintain themselves, change, grow or die; all these states are relevant to an understanding of resilience. Perhaps even more difficult—and interesting—to analyse are cases where a system becomes utterly transformed into something "new"; the dictatorial and post-dictatorial example may be seen in this light. The application of systems thinking to human affairs is typically done not only to *describe* social or political phenomena, but to contribute *prescriptively* to change and improvement in the latter in accordance with ideals and values that are, of course, themselves open to debate.

A system may not only react to environmental effects by changing its internal properties or organisation, but also act on and change its environment, bringing about a new relationship or a new equilibrium. Several "resilience" authors suggest this, and their observations are germane to current attempts to clarify the concept and make it relevant to contemporary debate and practical application, as we shall see. Holling, a leading theorist of ecological resilience, calls the two approaches "analytical" and "integrative" (Holling, 1998). White and O'Hare (2014) distinguish between "equilibrist" and "evolutionary" resilience; Longstaff's (2005, p. 27) similar distinction is between "engineering" (status quo maintenance) and "ecological" (state change) resilience; and Taleb's (2013) is between "antifragile" and "resilience". In the business context, Hamel and Välikangas's (2003) terms are "strategic resilience", involving "continuous anticipation", and "dynamic reinvention". More pessimistically, Walker and Salt (2006) note that "complex adaptive systems can…have more than one 'stable state'"; depleted fish stocks may not be resilient enough to recover (p. 36); and change may be slow and unnoticed (p. 10). Feibleman and Friend's (1945) comprehensive framework enables the location of resilience within a variety of stances that relate to the nature of the systems that respond to environmentally induced changes or stimuli.

In these approaches, outcomes may be achieved through processes that include communication, flows of information, learning (Deutsch, 1963) and awareness of the entity's internal state and of the configuration of its environment, and by means of instruments for discovering and for affecting salient parts of the external world (Hood, 1983). These may all be seen as part of a repertoire for being resilient in the face of threats, whether by anticipating and avoiding these risks or by responding when they occur. We cannot fully explore these processes here, or relate them systematically to resilience to surveillance. However, drawing upon such constructs and concepts helps in generating and answering important questions about the resilience of a social system—including its democratic values and practices—to adverse events, whether these be external or internally generated ones such as are posed by systems of mass surveillance.

Relating to the points derived from the examples described earlier, many questions could be posed, inviting deeper development of resilience strategies, and illustrating the way in which theoretical and conceptual analysis affords a purchase on the kinds of processes that are of particular interest to us in focusing upon the threat posed by the mass surveillance of communications in particular. However, space permits only a few basic questions here; these are prompted by high-level approaches but are deliberately re-orientated towards the political and social frame of reference in which we seek to analyse resilience phenomena. The current questions include:

- What analogies can be drawn from the processes of threat and responses in other concrete systems in order to model surveillance-resilient processes?
- Is the threat carried out suddenly or incrementally?
- What "constitutive public goods" are at risk in liberal-democratic societies, and what sustains them?
- Do resilient adaptations result in the maintenance or restoration of pre-surveillance levels of public goods, or is a new equilibrium established at lower or higher levels?

Further questions—not considered here—would include:

- How vulnerable are these public goods to the threat of surveillance?
- Can we describe, in equilibrium terms, the relationship between a liberal democratic society and the state(s) in its environment?
- How much (and what forms) of surveillance threaten what public goods?
- How severe is the threat, and what public goods-sustaining social and political processes and functions are threatened?
- What is the society's degree of flexibility and its potentiality to adopt one or another response to external threats?
- How does the system (i.e. society) learn about the potential threats to its public goods, processes or functions?
- Can democratic societies take anticipatory action

to prevent these threats from occurring or to mitigate their likely effect?

- What are the internal (re-)organisational and resource prerequisites to anticipatory and self-organising activity to prevent or mitigate threats?
- Does such action include only internal change in culture, structure and behaviour, or does it also include efforts to inhibit surveillance at source?

4. Modelling Resilience

We have already observed that there is now a sizeable and growing literature on resilience, featuring various definitions, though also some common conceptual language (Clarke, 2013). A document on food security defines it as "the capacity of agricultural development to withstand or recover from stresses and shocks and thus bounce back to the previous level of growth" (The Montpellier Panel, 2012, p. 11). Cognisant of that document, another one in the same field says, more generally: "Resilience is the ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks" (European Commission, 2012, p. 5). It continues:

> The concept of resilience has two dimensions: the inherent strength of an entity—an individual, a household, a community or a larger structure—to better resist stress and shock and the capacity of this entity to bounce back rapidly from the impact….It requires *a multifaceted strategy* and a broad systems perspective […and] calls for a *long-term approach* (European Commission, 2012, p. 5; emphasis in original).

Within academic literature, Chandler (2012, p. 217), for example, has defined resilience as "the capacity to positively or successfully adapt to external problems or threats". Writing from a more psychological perspective, Luthar, Cicchetti and Becker have similarly defined resilience as "a dynamic process encompassing positive adaptation within the context of significant adversity" (Luthar et al., 2000, p. 543; cited in Bourbeau, 2013, p. 7). Hall and Lamont (2013b, p. 13) define "social resilience" as "an outcome in which the members of a group sustain their well-being in the face of challenges to it". There has been some debate, however, as to what the nature of all these forms of resilience adaptation might be.

References above to the work of White and O'Hare (2014) and to Longstaff (2005) showed that one way to understand the nature of "resilience", and to distinguish between different kinds of resilience, is to consider whether the system reverts back to the status quo or instead changes to a new state. Similarly, the colloquial term "*bouncing back*" is often used to capture a quality of resilience, connoting recovery to the prior state of "normality". However, as Folke (2006, p. 259) has argued, resilience may also involve evolution towards a "new normality" or perhaps a new equilibrium, comprehensible in terms of the theoretical underpinning discussed above, and which one might term "*bouncing forward*". In a variant of the twofold distinction, Bourbeau (2013, p. 8) draws a threefold but perhaps broadly similar distinction, namely between engineering (equilibrist) resilience, ecological resilience (system continuity), and socio-ecological (emergent or adaptive) resilience. He then goes on to suggest a revised threefold distinction, namely between "resilience as maintenance", resilience as "marginal adjustments", and resilience as "renewal" or "remodelling" (2013, p. 12). Bourbeau consequently defines resilience "as the process of patterned adjustments adopted by a society or an individual in the face of endogenous or exogenous shocks" (2013, p. 10). Additionally, and presumably in order to distinguish the analysis of the workings of resilience from resilience itself, he proposes the new term "resiliencism", which he defines as "a conceptual framework for understanding how continuity and transformation take place under these circumstances" (2013, p. 10; see also Bourbeau, 2015a).

Another way of approaching the question of how best to define or characterise "resilience" is to identify the various different strategies or techniques it typically employs. An interesting feature of resilience strategies is that they seem to involve a combination of forward-looking measures attempting "to anticipate, prepare for, and, as far as possible, avoid the worst excesses of the next disruption" (Cho, Willis, & Stewart-Weeks, 2011); measures, such as resistance, designed to combat current events; and learning, recovery or change measures in response to adverse events that have already occurred. Moreover, it is clear that we need to distinguish between resilience as a *strategy* and resilience as a *description* of empirical reality. Furthermore, we agree with Bourbeau that, especially in relation to the second of these, rather than imagine resilience as being wholly effective or ineffective, it makes more sense to consider it as a matter of degree. In a subsequent section, we explore these various elements further and propose a framework within which various scenarios can be modelled, including ones that are not normally entertained in discussions of resilience, namely where it fails. Before that, however, we turn to a brief discussion of the differences but also the relationships between resilience and resistance.

4.1. Resilience and Resistance

Resilience is not a one-off performance, but a sustained and systematic process that includes capacity-building institutional and procedural development. It partly overlaps with "resistance", an important but relatively unexamined concept in surveillance studies, involving individual and group opposition, protest, and defensive measures, but is a quite different process and not synonymous with it (on the issue of "resisting surveillance", see Bennett, 2008; Fernandez & Huey, 2009; Introna & Gibbons, 2009; Lyon, 2003b; Martin, Brakel, & Bernhard, 2009; Sanchez, 2009; Wells & Wills, 2009; Wright & Kreissl, 2015). In relation to the opposition to surveillance, privacy and other human-rights advocates might ask why the adoption of "resilience" terminology and frameworks should be preferred over existing discourses and strategies involving "resourcefulness", "risk management" and, in particular, "resistance". Evans and Reid (2013) lament the conflation of "resilience" and "resistance". They abhor the de-politicisation of "resilience" in which individuals are exhorted to abandon resistance and to adapt to, rather than to oppose or politically transform, situations of insecurity and adversity. They see this as a "nihilistic" capitulation to liberal regimes that thrive on the insecurity of others.

Although we do not share these authors' confidence in "resistance" as the preferred stance, we fully acknowledge the many overlaps and linkages between it and "resilience". However, we seek to demonstrate that the conceptual and practical apparatus of resilience identifies various discrete components that might also inform future *resistance* strategies; it offers a distinctive holistic approach of a kind not always readily captured in the notion of "resistance". Moreover, in some languages, "resilience" does not have a straightforward equivalent. But even where there exist separate terms for resilience and resistance, actions aimed at withstanding shock-like adverse events can have a resistant and resilient aspect alike. According to popular conception, resistance can be associated with a rigid entity that undertakes an aggressive or even counter-striking action to defend itself, while resilience may evoke more flexibility, as systems theory indicates. In many cultures, and in the history of oppressed peoples, heroism demands resistance. In other cultures and movements, "passive resistance" or "turning the other cheek" are the principled and valued responses. Sometimes, there may be a dramatic choice.

At a general level, although both notions incorporate elements of prediction and prevention, resistance can be seen as a response that concentrates on the present; tries to avoid changes and preserve the existing state; emphasises the political dimension of the struggle; and sometimes uses radical solutions such as pre-emptive strikes or self-destruction. Resilience, on the other hand, refers to a broader and sometimes more bureaucratic range of measures deployed to try to cope with changes, and that may learn from the past and plan for the future as well as deal with the present. Thus the resilient entity is not only able to recover but also to develop ways to exist within adverse circumstances, and also to prevent future adversity.

Bourbeau (2015b, pp. 17-18) has recently suggested a further way in which resilience and resistance, while different, are interrelated, namely that the capacity to resist, especially on an on-going basis, might be thought to require some resilience capability as a prerequisite for success. For example, the capability to mount resistance strategies could be seen as reflective of an entity exhibiting resilience; and the ability to withstand and bounce back from the likely setbacks involved in a resistance struggle also seem "resilience-like". Lastly, a successful resistance measure may even lead to a new state of affairs, or "bouncing forward".

The question of process also points towards resilience's inclusion of a *learning* component, another complex matter to be explored. It is one of the steps in a temporal sequence that is recommended for building resilience in a specific domain such as agricultural development, and in wider policy discourse. This includes activities to *anticipate*, *survey*, *prevent*, *tolerate*, *recover*, *restore* and *learn*. As we will soon see, a resilience model used in the agricultural development field (Conway, Waage, & Delaney, 2010, p. 309) is helpful because it neatly summarises the content of resilience processes and offers a dramatic visual representation of what may typically take place over time. Other terms used in the agricultural setting are *withstand, resist, handle, absorb, adapt, response, resume, optimise, innovate, reconstruct, renew, and persist.* In the field of disaster-reduction, the concept of *vulnerability* is also important: "[t]he conditions determined by physical, social, economic, and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards" (International Strategy for Disaster Reduction (ISDR), 2004, p. 16).

Armed with such process-related terms, it is possible to model an approach to resilience to surveillance drawing upon such terminology to depict a continuous process embracing:

- anticipatory, preventive measures to mitigate the harms that may be brought about through surveillance;
- measures to absorb, resist or withstand the threats posed by surveillance; and
- post-event measures to recover and to learn how better to anticipate and/or to cope with harmful surveillance.

How the concepts are configured into relationships and sequences is a crucial question that will be sketched later on, but the details of this must be left for another time. Whilst these high-level concepts apply generically to situations of resilience, it is necessary to develop models that correspond closely to the circumstances of the different domains of application, but—again—detailed demonstration must be deferred. For example, some of these domains afford greater possibilities of anticipation and prevention than do others, and the part played in resilience respectively by society and by state institutions will also vary.

4.2. The First Step: Identifying the Components of Resilience

In this section, we explore some different sequences of adverse events and system responses, in order to highlight various possible outcomes in which a system does or does not exhibit resilience. Our discussion begins by taking a model from a particular domain, then generalising it, before considering its applicability to the question of societal responses to mass surveillance systems specifically. We use a series of diagrams to help illustrate the processes at work.

The heuristic diagram in Figure 1, drawn from work on agricultural development (Conway et al., 2010, Figure 9.9), shows a simple resilience sequence.

We will supersede this diagram with ones that consider surveillance as the disruptive phenomenon, but it is useful to refer to it and its definitions in showing the general, cross-domain conceptualisation of resilience—involving both preparedness and response[2]—and the part played by the concepts "stress" and "shock". In this construct, "stress" is defined as "a regular, sometimes continuous, relatively small and predictable disturbance", and a "shock" as "an irregular, relatively large and unpredictable disturbance" (The Montpellier Panel, 2012, p. 11), although it would be advisable to disaggregate each definition in order to show differences in size, predictability and continuity. The terms indicated in the x-axis, from "anticipate" to "learn", signify different activities that are important in resilience, albeit not necessarily in a clear sequence.

However, as this diagram derives from a developmental context, the expectation of a rising slope, especially as the target for recovery, cannot be simply transposed to a model tailored to a surveillance-and-human-rights context, because it is not obvious that rights protections can be confidently expected, or planned, to improve steadily over time. Similarly, from the perspective of surveillance and rights, the upward slope may indicate an ambiguity, namely whether the model represents an *ideal* (that it is desirable for "development" to increase over time) or whether it purports to represent *reality*, albeit abstractly (that societies typically are developing over time). Usefully, the diagram does not show only the course of a relatively simple "bounce-back", perhaps through some meandering, to the trajectory of development, but also envisages possibilities of indefinitely longer drift to lower levels where loss—de-development—replaces recuperation; in other words, the system has failed to be resilient.

We particularly recognise the potential of the concept of "resilience" to become, as Béné, Godfrey Wood, Newsham and Davies (2012) put it, a "form of integrating discourse" able to rally an "increasing number of people, institutions, and organisations under its banner, as it creates communication bridges and platforms between disciplines and communities of practices, and offers common grounds on which dialogue can then be initiated between organisations, departments or ministries which had so far very little, or no history of collaboration" (p. 12). Such bridges and platforms are crucial to countering the detrimental effects of surveillance, ensuring effective respect for public goods and at the same time protecting people and communities.

[2] Conway et al. (2010) identify and diagram a further important element, "countermeasures", representing the deployment of measures to address the negative consequences of stresses or shocks that have become apparent (Figure 9.8). The effectiveness of countermeasures is not assumed, and subsequent scenarios, for better or worse, can then be sketched.

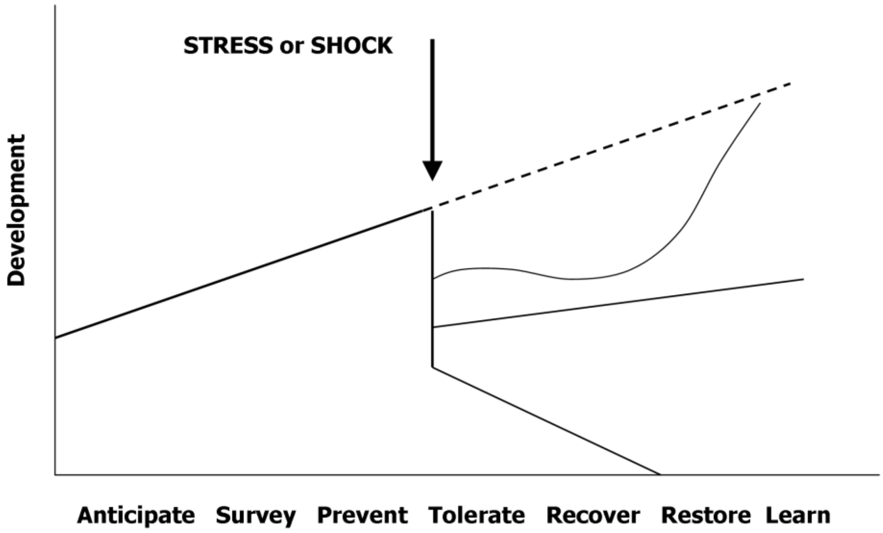


Figure 1. Agricultural development model of resilience. Note: A similar diagram was used in IRISS Deliverable 6.1, and was adapted from The Montpellier Panel (2012, p. 11).

4.3. The Second Step: Developing and Exploring the Resilience Framework

With this in mind, we take further steps in the direction of resilience to surveillance by means of revised models. Figure 2 depicts two axes: public goods, and time. The x-axis is re-labelled "time" because this makes explicit what is implicit in the original model, namely that the diagram represents a *temporal flow*, and that its constituent elements (anticipate, survey, etc.) may be thought of as associated with different moments in relation to the stress or shock event. The y-axis is re-labelled "public goods", in order to generalise the model's applicability. Loader and Walker (2007, p. 145) argue that an expanded concept of "public good" can usefully be applied to the study of security by including not only shared societal goods such as liberty or freedom of expression, but additionally, by seeing such a good as a "constitutive public good"; that is, a societal good understood as an integral and essential element of society itself. We contend that this expanded concept can similarly be applied to the study of resilience in general, as well as to privacy in particular when it is threatened by, for example, "national security" surveillance. Public goods can refer to any "good" of potential fundamental benefit, but here we are particularly interested in goods relating to freedoms, liberties, rights, democracy, security and privacy: the ones that are typically impacted by surveillance. A further advantage of using the term "public goods" is that it can refer both to their realisation in practice, and the vigour with which they are valued as societal values.

In Figure 3 we introduce a new element, the "ideal level" of the desire for, vis-à-vis the "real level" of public goods. We represent here the ideal level (i.e., how much a public good is desired or valued by society) as a horizontal line, hypothesising an ideal Western constitutional democracy where the desired level of public goods is constant. We also label the three scenarios represented in the original model (full recovery, partial recovery, and non-recovery).

As noted above, while there are some similarities between the concepts of "resistance" and "resilience", there are also important differences. Our revised model enables us to illustrate this distinction through a separate abstract model for resistance, which helps to distinguish it from the various cases of resilience (Figure 4).

Whereas Figures 1–3 model resilience in the face of the occurrence of a single major event, Figure 5 models resilience both in the face of incremental, "creeping" threats to public goods, as well as in relation to a single major event or a small but culminating event that "breaks the camel's back". Figure 5 thus better models resilience in relation to surveillance, in which surveillance threats may be incremental and gradual, or sudden and dramatic, although these properties are not unique to surveillance as a threat. It should be noted, therefore, that the model in Figure 5 is a general one, potentially also applicable to the threats to security that give rise to surveillance. It is possible to make advances on this diagram through other ones that depict further dimensions of resilience to surveillance, and that highlight other important considerations and questions about the path of resilience that pertain not only to the surveillance context but to others as well.

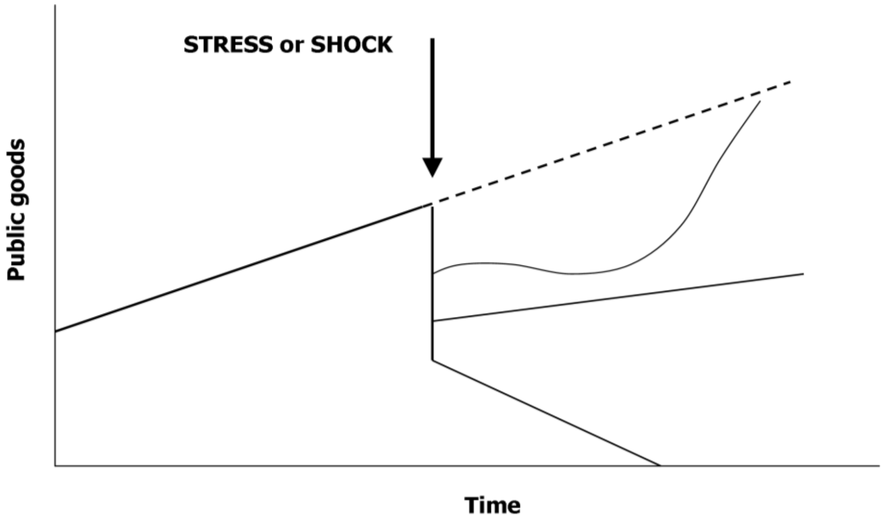


Figure 2. Relabelled Conway diagram.

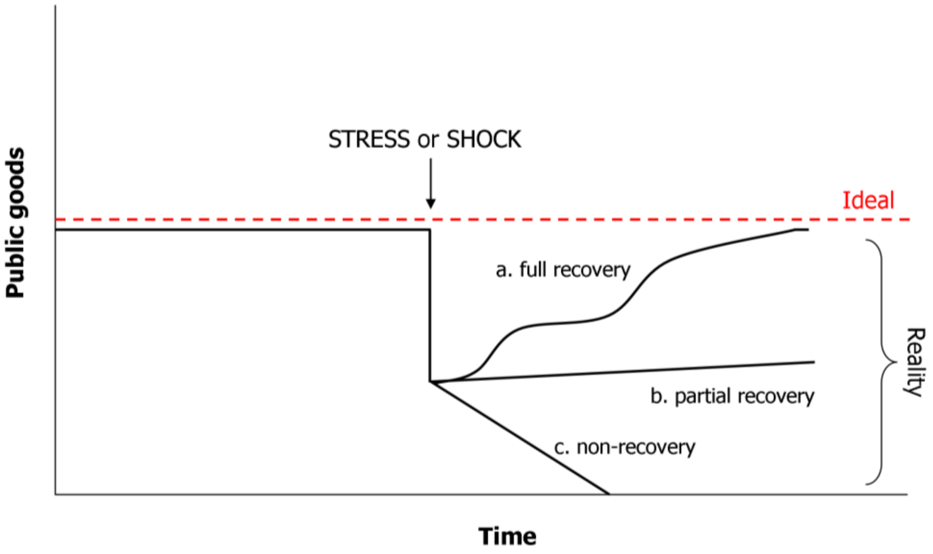


Figure 3. Modified resilience model.

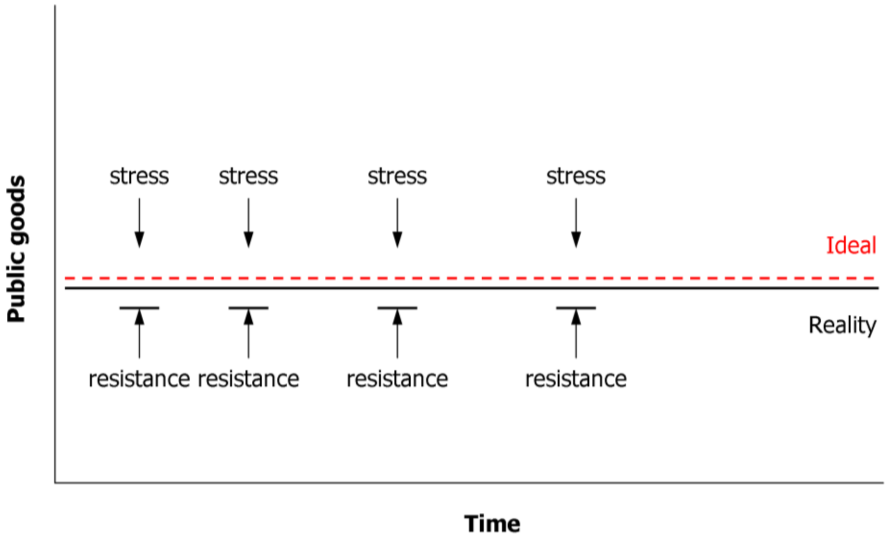


Figure 4. Resistance towards stresses and shocks.

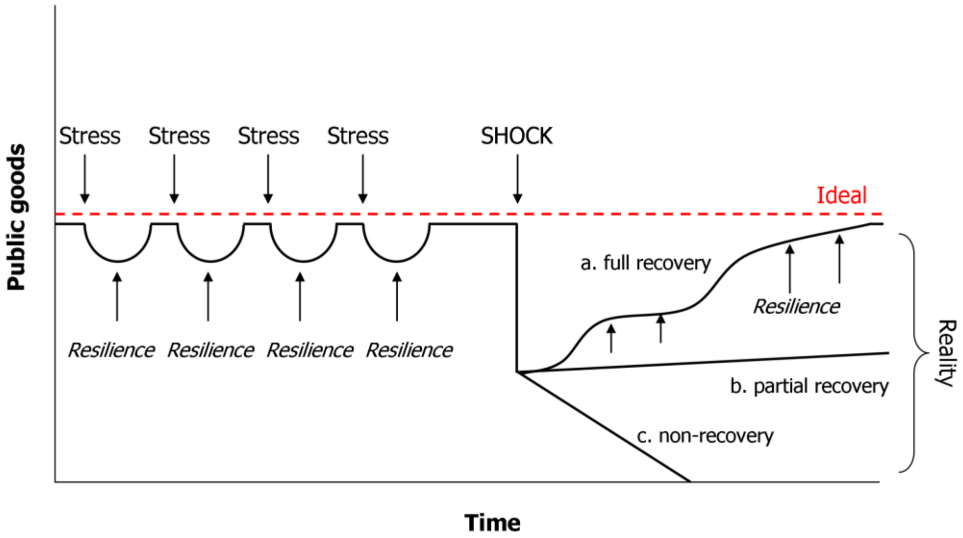


Figure 5. Resilience towards repeated stresses and shocks. Note: An earlier version was used in IRISS Deliverable 6.1.

In the case of security or agricultural development, stresses or shocks are often modelled as sudden major shock events, for example, a terrorist attack or famine. However, in the case of surveillance, measures introduced that have a deleterious effect on civic society, such as a "chilling effect" on political debate or freedom of assembly, need not be singular or sudden, but may instead be smaller but more sustained. Consequently, this diagram incorporates an additional resilience scenario, showing a *series* of stresses, each one followed by an episode of resilience, which in the paradigm case restores the public good in question to its prior state, although of course full restoration need not be the case. The diagram also shows a final stress or shock—whether small or large—that has a larger effect on public goods, so that resilience has a more uncertain outcome and may take longer. As in agricultural development, the uncertainty of the outcome is shown by the top line following the "final" stress or shock, and by two further lines that represent the re-establishment of public goods at reduced levels. For the sake of simplicity, the public goods are depicted as fully restored after several stresses prior to the ultimate stress or shock, but other trajectories are possible: one in which the public goods are eroded over time (the line descends); or alternatively where public goods are actually enhanced (the line ascends; to be shown later).

4.4. A Closer Look at Resilience Elements

It is not the aim of this article to produce an ultimate, universal definition of resilience, nor to vote for one of the existing definitions (and consequently approaches) from the wide spectrum between specific application areas and the view of Neocleous, who dismissively says that resilience is "all and everything". Nevertheless, in order to understand better the notion of resilience in general and in the context of surveillance, we need to explore its fundamental elements and their reasonable spheres of interpretation, and to highlight at least the most important aspects of these elements. We focus on three such elements: the reference point or *normalcy*, the *time scale* in which changes can be measured, and the role of *perception*.

4.4.1. The Reference Point or the State of Normalcy

As has been shown, resilience is generally understood as a "good thing", an entity's positive capacity or strength that enables it to resist stress and shock or to bounce back from the impact. Consequently, stresses and shocks are considered in this context as adverse impacts or events: "bad things" that degrade the original state of the entity. Although in this article we regard resilience as potentially positive, resilience as an abstract notion is inherently value-neutral. Every structure or entity can have the characteristics of being resilient towards external or internal impacts. It is relatively easy to identify those states of entities that are widely regarded as having positive value, while the stresses or shocks to it are seen as negative, and towards which the entity should be resilient. For example, most people would regard food safety as a beneficial state of society, and see floods and droughts as having adverse impacts. It is regarded as positive if the system can mobilise food reserves, thus being resilient towards such impacts. Similarly, there is consensus that a working electricity, waterworks or telecommunication infrastructure is a "good thing". Our war enemies' resilient infrastructure is regarded as a bad thing from the standpoint of our interests.

Even if we consider resilience from our own perspective and interests, in reality most beneficial states are not optimal; the ideal state might only be expected or imagined. However, it is possible to evaluate changes and resilient responses in relation to these sub-optimal states, too: in other words, to measure the level of resilience in relation to these realistic situations. If a country's food safety is not optimal, but can bounce back from even the strongest of shocks to the usual, sub-optimal level, it can still be regarded as resilient.

Society as a whole or the groups that constitute it cannot be regarded as homogeneous entities with regard to either the positive or negative nature of the state of normalcy or to the positive or negative nature of the stresses or shocks, as the example of dictatorships showed. For most individuals or social strata a strong stress or shock, such as an economic crisis, can be adverse, yet for others it could be beneficial. This may have a strong impact at a higher level of society, too: it may change power relationships and the social distribution of goods. In such contexts, the formal or informal obligation to be "resilient" may easily be abused or at least used in a questionable manner (Slater, 2014). Since we focus on the social implications of resilience, we adopt the values (public goods) of western liberal democracies. But even within this value system, the same impact may have both beneficial and adverse effects on the same citizens concerned, an example of which is the consequences of ubiquitous surveillance in the developed world.

Finally, the reference point (or reference line in the graphical models, below) is not always stationary: it is changing, even if change cannot easily be perceived because of its slow pace. In addition, the inherent public goods—reflected in the written and unwritten norms governing the life of a social entity—may also change as a result of repeated stresses or shocks. Figure 6 shows an expanded model of resilience with eroding public goods. The vertical axis, "public goods", refers both to the horizontal line that shows the persistence of a good's desirability (the "ideal"), and to the descending line that shows the decline in its reality under conditions of stress. As our introduction remarks about surveillance suggested, this situation is quite realistic in an environment where citizens become resilient towards security threats but gradually lose their "reasonable expectation" of privacy, autonomy, or dignity due to increased surveillance.[3]

However, it is also possible that repeated stresses and shocks result in an enhanced desire for public goods, perhaps through an increase in social solidarity, institutional organisation, morale, greater awareness, or other reinforcing conditions and factors. Thus citizens may become sensitised to the detrimental social side-effects of security measures and increase their demands regarding the guarantees of their privacy, dignity, autonomy, etc. in such situations (Figure 7).

Resilience towards security threats may also mask adverse changes affecting certain social groups, or conserve a social-political situation that is far from ideal and prevent it from improving. For example, increased social sorting—a possible adverse consequence of ubiquitous surveillance (Lyon, 2003a)—may be legitimised by the needs of resilience towards security threats and stresses. It is in the face of such challenges that societies may seek to affirm the principle that in a democratic regime even the positive aspects of resilience should not serve as a means to conserve contradictory social or political constructions or inhibit the development of a democratic, rule-of-law society.

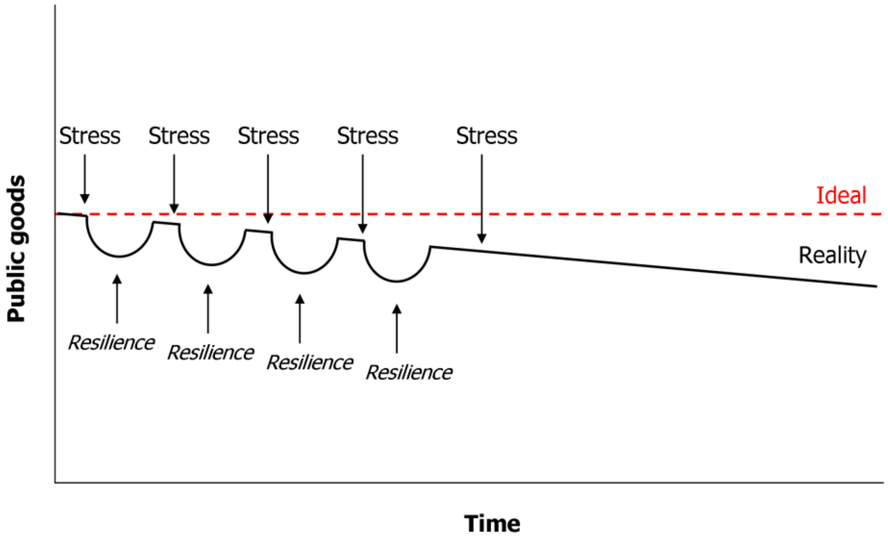


Figure 6. Expanded resilience model showing creeping erosion of public goods.

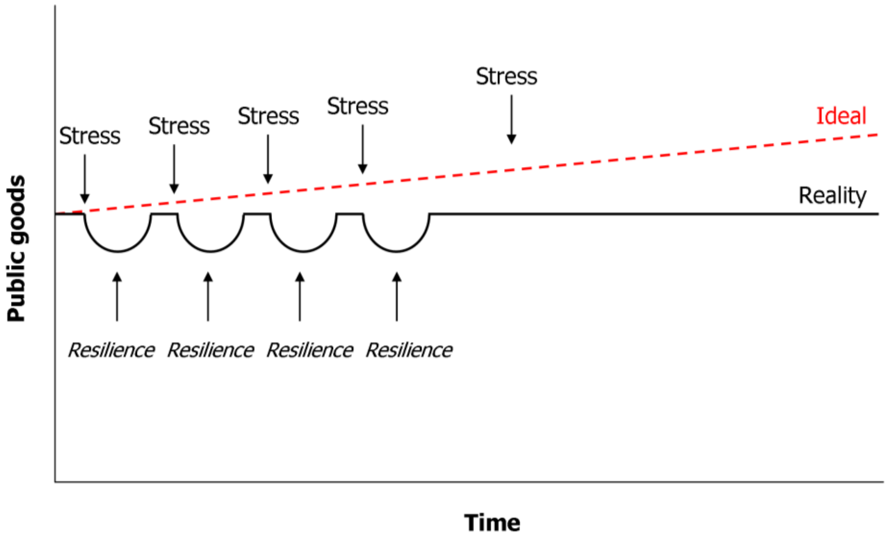


Figure 7. Expanded resilience model showing enhancement of public goods.

[3] With regard to privacy, the doctrine of "reasonable expectation", a complex and legally controverted concept involving both normative and empirical dimensions as well as contextual understanding of what is "reasonable" in what circumstances (Nissenbaum, 2010, pp. 233-236; Solove, 2008, pp. 71-74) is closely related to the level of public goods depicted in our diagrams, including increases and decreases over time.

4.4.2. Time Scale

The time dimension in the context of resilience is important from two main perspectives. First, if the intensification of stressful adverse changes is too slow to be perceived by social groups or individuals, the impacts will hardly be recognisable; thus we can speak about non-conscious, "instinctive" resilience only (see also the role of perception, below). Second, if the adverse impact is shock-like and therefore recognisable, but if the bouncing-back (or forward) phase is slow or uneven, the effect of resilience cannot be easily recognised. Two types of this second situation can be noted. In the first type, the impact is strong, its consequences are evident, and the recovery also consists of fast but only partial actions; full recovery takes a long period of time. The second type can be observed in the case of long-lasting emergency situations, such as wars or long-term natural disasters. Here the period of stresses and shocks lasts long but the recovery phase even longer; years may pass until one can conclude that society has regained or improved upon its earlier state.

However, if the original state of the society or entity will be restored or surpassed only after several years, or in the life of a new generation, it is debatable—in general systems terms—whether this can be regarded as a new entity, a new chapter in the history of the society, or as still part of the resilience capacity of the original entity (Braybrooke & Lindblom, 1963). In such situations, therefore, it is necessary to identify those public goods that, even in a changed environment, may represent the ideals with regard to which a society may be considered resilient. In this respect, a post-war country where the economy has been quickly restored, coupled with a dictatorial political regime, can be regarded as resilient in terms of the economy but not in terms of the society or polity, if the country had been a pre-war rule-of-law democracy.

4.4.3. The role of Perception

Adverse developments and their impacts, especially in the case of persistent stresses such as ubiquitous surveillance, may remain unnoticed by those affected. When they finally realise the consequences, the moment for diminishing the impact or developing an alternative strategy may have passed. Such a situation may also result in an unnoticed erosion of the "ideal" level of desire for public goods, as shown in Figure 8. The widely used metaphor of the boiling frog is illustrated here and in Figure 9; it refers to the ability or inability of people (or any entity) to recognise and react to important adverse changes that occur gradually.[4] The boiling frog metaphor has been suggested before in relation to surveillance (Marx, 1987, p. 54), and it can also be understood as representing what a former UK Information Commissioner once famously termed "sleepwalking into a surveillance society" (Ford, 2004). The issue of perception may relate to that of timescale; for example, adverse changes taking place gradually over a long period of time may be much harder to perceive than a similar aggregate change taking place over a much shorter time period.

On the other hand, even in a successfully resilient construction, the actors themselves might not be fully aware of their own resilience activities. In other words, there exist perceived shocks and stresses, and unperceived ones, coupled with conscious resilience options and unconscious ones. The possible combinations are manifold. In such situations and also on a societal level, the observer can identify an important moment: the moment of perception (Figure 9).

[4] See http://en.wikipedia.org/wiki/Boiling_frog

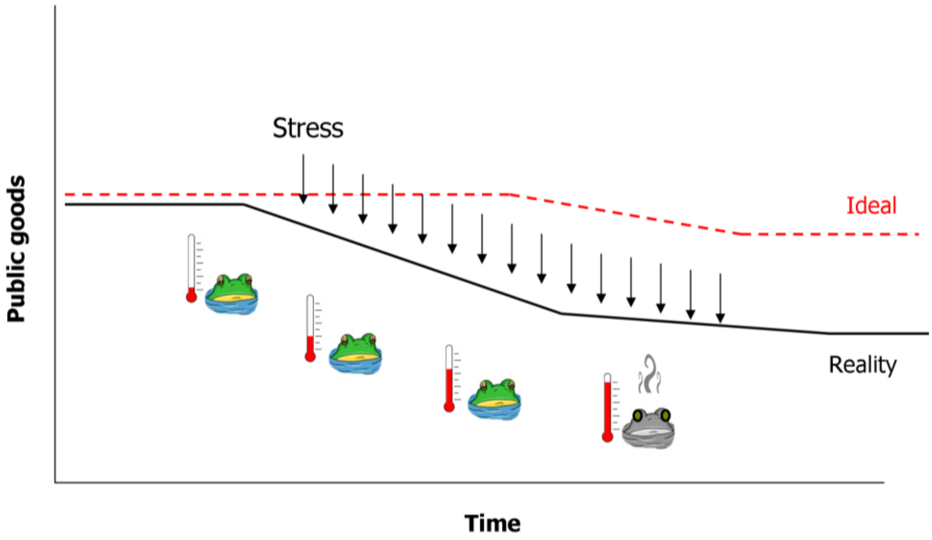


Figure 8. Unperceived stresses and eroding public goods.

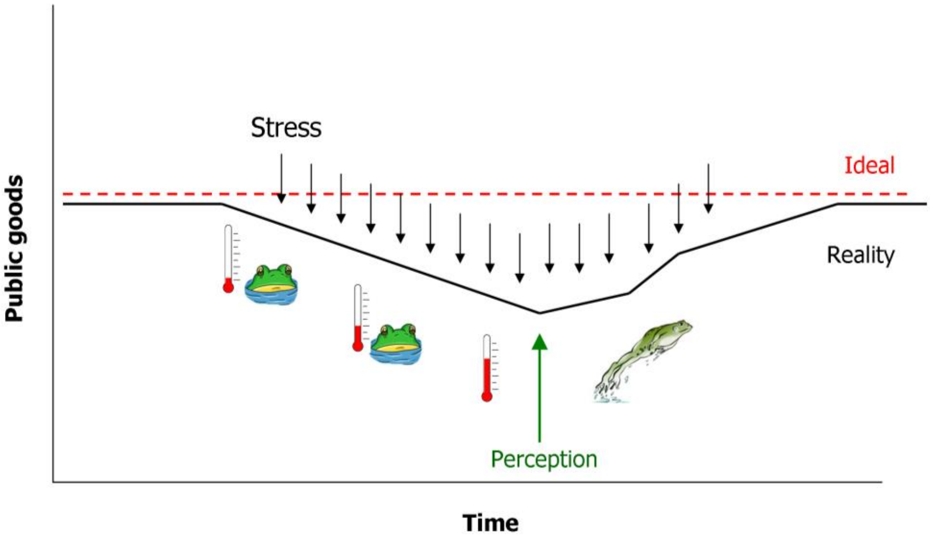


Figure 9. Perceived stresses and chances of resilience.

This diagram depicts a scenario in which the moment of perception prompts action leading to a change of real conditions. However, another scenario (not depicted) could show a case in which it is not possible to change real conditions, so that the moment of perception leads instead only to an increased desire for an "ideal". This can have special importance in the surveillance domain: surveillance stresses, even shocks, are often not perceived by the affected population, not to mention the indirect consequences of such impacts. For example, until the 2013 Snowden revelations of mass surveillance, people in Western societies were only dimly aware of, or even oblivious to, the fact that they had far less communications privacy than they had thought or had reason to expect. The public's valuation of privacy has arguably increased as a consequence of this new awareness. Aradau (2014, p. 79) uses the term "moment of surprise" to describe the moment of perception (which may be experienced immediately in the case of shocks, or belatedly, as here, in the case of incremental stresses). Indeed, she argues that resilience approaches have become popular in policy fields precisely "as a response to the problem of surprising events" (2014, p. 87).

5. Resilience in the Surveillance Context

We have argued that much contemporary surveillance, and its effects on public goods, is predicated upon policies and practices aimed at promoting the security of states and societies. In the field of security—which is close to our concerns in thinking about surveillance—"resilience" has tended to be used in the sense of "resilience to terrorism/subversion", and the concepts and strategies used are drawn from the lexicon mentioned above. Here we propose to explore how similar resilience mechanisms might be employed to make societies more resilient to the more negative consequences of the state and corporate surveillance that is undertaken in the name of security. However, in doing so, it becomes apparent that certain assumptions of the existing resilience models/paradigm must be called into question. Developing a resilience framework to incorporate different assumptions indicates that various outcomes are possible. We conclude that not only does this suggest that the use of a resilience strategy in opposing greater surveillance should be adopted with only limited optimism, but that our analysis highlights the limits of such resilience in general, including in relation to improving security.

We now take this third step in the modelling of resilience, narrowing down from the general and abstract to consider specifically resilience to *surveillance* itself as the source of stress. The original Conway et al. (2010) model suggests a way of conceptualising different strategies to oppose or resist surveillance, namely along the broadly temporal sequence of anticipate, survey, prevent, tolerate, recover, restore and learn. Rather than simply reactively opposing insidious surveillance programmes when they are initially proposed or revealed, a "resilience"-based approach suggests that, additionally, it would be beneficial in advance to prepare a raft both of preventive measures and restorative contingency measures.

From this perspective, specific measures that could be deployed to oppose surveillance can be seen as potentially involving a number of these strategy qualities. For example, the establishment of constitutional or human rights legal protections are in part anticipatory (because they anticipate future governmental attempts at their encroachment); in part preventive (because a constitutional court might rely on such provisions to strike down a proposed new law as unconstitutional); restorative (because higher constitutional courts may be acting sometime after a law was originally introduced); and exemplify learning (because jurisprudence may develop in the light of new technologies, their capabilities and implications for citizens). Similarly, citizens' use of encryption techniques to protect their personal communications may be anticipatory (of unknown future attempts at their interception); preventive (preventing immediate disclosure); restorative (introduced specifically to reinstate effective privacy in the light of recognition of its former weakness); or demonstrate learning (the adoption of even stronger cryptographic systems in the light of revealed weaknesses).

The second respect in which this analysis of resilience potentially informs overall strategies for curtailing surveillance is that the area of surveillance itself prompts us to question many of the assumptions underpinning conventional models of resilience. As a result, our analysis suggests that considerable caution is warranted and that resilience strategies are no panacea. Snowden's revelation of mass Internet surveillance programmes may present as a sudden major societal shock, and be met with resistance or recovery processes of certain kinds that could reasonably be characterised as "resilience". However, this surveillance, deployed gradually and stealthily for many years, went unnoticed and unchallenged (see Figures 8 and 9). Moreover, it remains to be seen whether future governmental mass surveillance programmes will successfully be constrained, given the temptations they may offer, the vested interests in the intelligence community, and international as well as national considerations. Furthermore, we may also speculate that societal valuing of privacy may have become eroded rather than reinforced as a result of the recent disclosures, leading to a resigned acceptance of the impossibility of truly private personal communications in the digital age.

The diagrams below illustrate, in a unified structure, both security- and surveillance-related stresses, as well as resilience responses towards them. Figure 10 shows the adverse impacts and the resilience responses reflecting the traditional trade-off model between security and privacy: the trajectories of these two public goods are shown within the diagram. This model presupposes that, with regard to their privacy implications, citizens evaluate the introduction and use of security/surveillance technologies in terms of a trade-off; in other words, they regard such situations as a zero-sum game: more security equals less privacy and vice-versa. This popular hypothesis implies that, under threats to security, security will trump privacy. The diagram also shows the presupposition that surveillance measures are natural consequences of terror and other threats to security, thereby representing stresses of their own, too, in a chain-like pattern.

Recent research challenges the universal validity of this trade-off model and criticises its use in legitimising the introduction of privacy-invasive security technologies. Empirical studies investigating people's perception and attitudes in this area indicate that people regard security and privacy as two separate public goods, and that they want both simultaneously.[5] In such a model both remain unchanged during stresses and shocks of both types; in an ideal situation, as a result of resilience responses towards both types of stress, the real situation remains unchanged as well (Figure 11).

[5] Most significantly the PRISMS project, (The PRIvacy and Security MirrorS): "Towards a European Framework for Integrated Decision-Making", Project No. 285399, 7th Framework Programme of the European Commission.

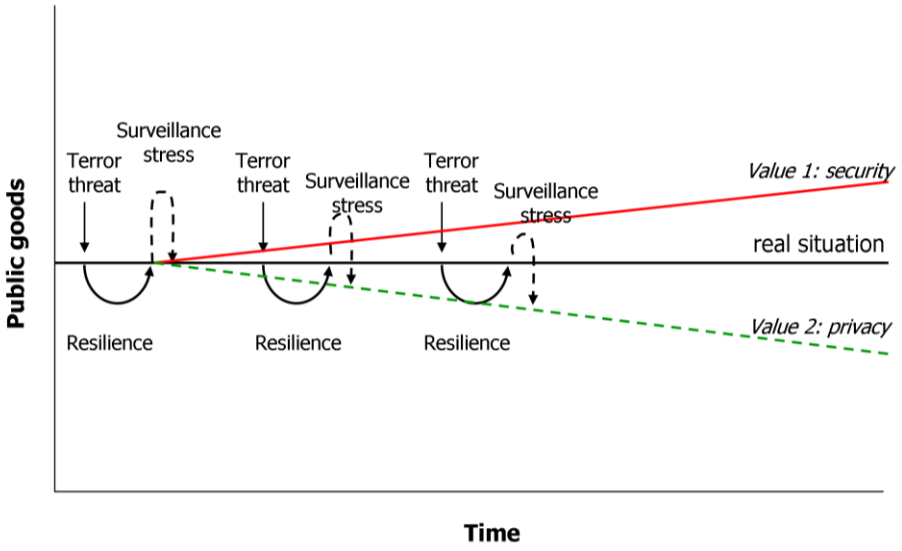


Figure 10. Terror threats and surveillance stresses in a security/privacy trade-off model.

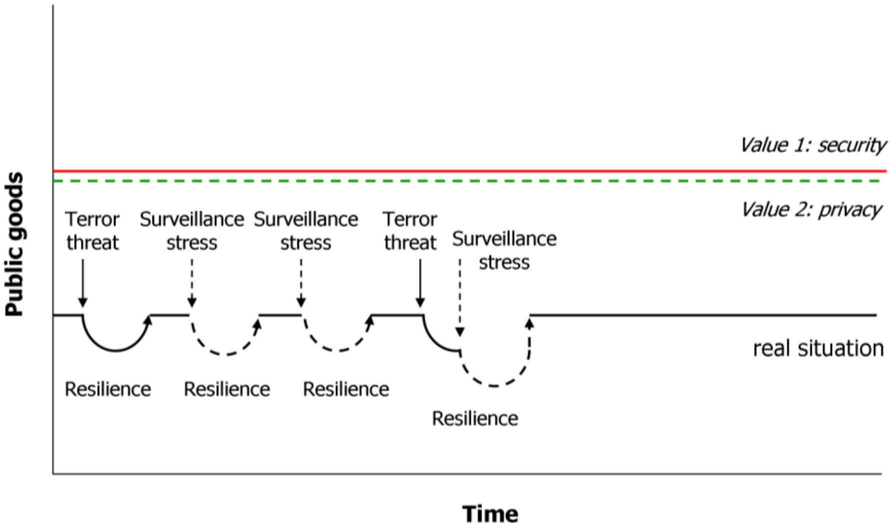


Figure 11. Terror threats and surveillance stresses in a separate public goods model (ideal situation).

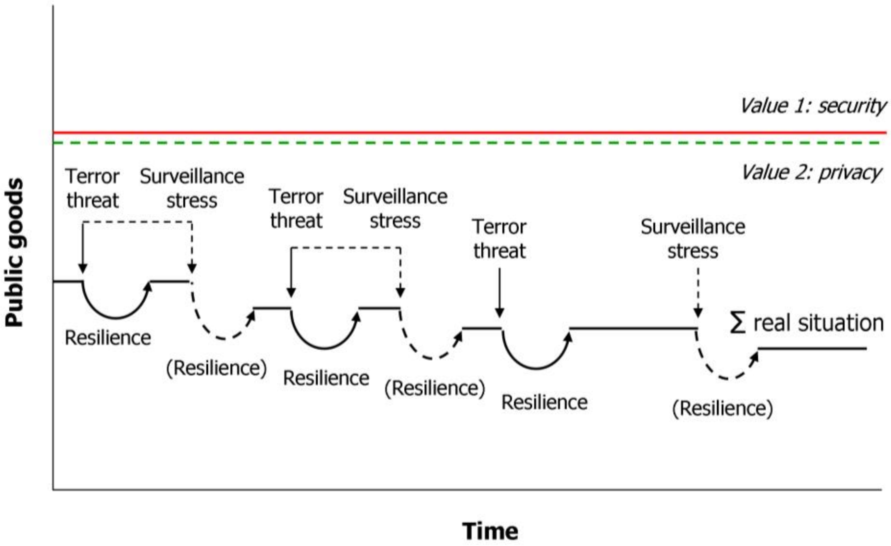


Figure 12. Terror threats and surveillance stresses in a separate public goods model (observed situation).

However, even if the society or a substructure is resilient towards security threats and shocks and bounces back to the original state of normalcy, this may not be reflected in the context of surveillance: the negative consequences of surveillance—such as increased social sorting, detrimental effects upon the social capital of interpersonal trust and social solidarity, or the erosion of privacy—result in worsening the summation (Σ) of the two components of the real situation, as illustrated in Figure 12. This figure usefully helps visualise that the public goods of security and privacy may indeed continue to be held in high esteem, but that this may nonetheless mask the gradual erosion in the real situation of citizens" enjoyment of these public goods.

6. Conclusion

There are a number of benefits of creating a general framework for the modelling of resilience, both in order to understand better the capabilities and limits of resilience approaches in general, and in order to model the threats posed by surveillance in particular. First, it helps both to organise existing knowledge, and to indicate gaps; second, it shows the relationship between, and ways of integrating, different resilience instruments; and third, the model can be applied at many different levels, from the local to the global. Such models consist of concepts that together describe, abstractly and schematically, what it means to be resilient in a host of specific contexts and applications. We have focused upon one context: surveillance for the purpose of (national) security.

It could be argued that elements of a strategy of resilience in the face of threats posed by surveillance are already to be found. Civil liberties and Internet privacy groups regularly campaign against government proposals for new legislation introducing surveillance measures, which we could understand as "resistance" activities. Many countries afford protections to their citizens in respect of fundamental rights, whether by means of constitutional provisions, international treaty obligations, privacy laws and other instruments (Bennett & Raab, 2006), which could be understood as, in large part, an anticipatory or preventive resilience strategy against possible future governmental attempts at their erosion.

Our argument here is that, in two respects, attending to the notion of resilience is useful in understanding the prospect of societal "pushback" in the face of greater surveillance. The first is that it potentially offers surveillance activists a framework for developing a wider range of measures and tactics for opposing surveillance. However, second, and more directly the focus of the present article, is that while the notion of resilience brings with it a consideration of anticipatory, immediate and future responses, it encompasses an unspecified and hence ambiguous time-frame of analysis, which could various refer to the short term, medium term, and even perhaps approach the *longue durée*. This is why the horizontal axis of the diagrams, and the vertical axis for that matter, are not calibrated to show intervals or magnitudes. Beyond the weeks, months, or few years in which we are accustomed to reckon the span of events, the unfolding of resilience—including the habits, outlooks, myths and stories, and institutional changes—that takes place in societies and cultures may follow a trajectory that encompasses many generations: historical time, not journalistic time.

The terminology of resilience has tended to be associated with strategies to enhance security, including the possible deployment of further state-surveillance measures. As a consequence, "resilience" as a concept has tended to be viewed as associated with securitisation processes evaluated as "good". However, this article has argued that, in the abstract at least, resilience can be regarded as neutral, and that its evaluation is a consequence of its application. Moreover, since "resilience" is an umbrella concept gathering together a range of measures designed to thwart an undesirable challenge or to remedy its effects, it offers a way of unifying such individual measures into a coherent strategy. Since it both suggests a concrete framework for developing policy and describes a desired on-going quality of a successful scenario, a repurposed application of the concept suggests ways in which democratic societies might become more resilient to the threats posed by surveillance itself.

This perspective is particularly useful in helping to understand different societal responses in the face of attempts at surveillance expansionism over time. This is because it enables us to model and explore different scenarios and outcomes—still, of course, to be elaborated and then tested empirically—including those in which surveillance measures expand to the detriment of public goods, and hence in which resilience to surveillance may be said to have failed. As such, and unlike many previous models of resilience, the models presented here do not assume resilience strategies always to prove successful. The diagrammatic representation of resilience prepared by Conway et al. (2010) represents a significant advance over the "optimistic" versions of resilience policy often informing resilience strategies, insofar as it acknowledges the possibility of negative outcomes (a "failure" of a system to prove itself "resilient"). However, the diagram is ambiguous as to whether it represents a normative goal or a description of a state of affairs. By separating these two qualities, we have been able to offer different scenarios involving interactions (but also divergences) between the two. As well as offering a cautionary note as to the likelihood of success of resilience-based strategies in *opposing* surveillance, an implication of the analysis presented here is that governments and authorities should be similarly circumspect regarding the efficacy of counter-terrorist and other state security resilience strategies, including the *imposition* of surveillance, since the same limitations apply.

Crucially, this article has contended that whilst surveillance strategies may (ironically) be deployed by societies in the name of greater "security", surveillance measures may have significant long-term detrimental consequences for constitutive public goods such as privacy, and hence be detrimental to society more generally. Whereas it has long been noted within surveillance studies that surveillance may produce a "chilling effect" on social and political debate, our analysis has identified more long-term, but no less insidious, consequences of increased surveillance of citizens, and this has to be taken into consideration in the fields of security studies and resilience studies alike.

Acknowledgments

Some of our thinking about surveillance and resilience took shape within the European Commission's FP7-funded project on Increasing Resilience in Surveillance Societies (IRISS), EC Grant Agreement No. 285593, 2012–2015. We are grateful for comments by IRISS colleagues in conferences and lectures organised in 2014 by the Surveillance Studies Network, by King's College London, and by the Eotvos Lorand University (ELTE) Faculty of Law.

Conflict of Interests

The authors declare no conflict of interests.

References

Aradau, C. (2014). The promise of security: resilience, surprise and epistemic politics. *Resilience: International Policies, Practices and Discourses*, *2*(2), 73-87.

Ban, K.-m. (2009). Resilience and solidarity: Our best response to crisis. Address to the 62nd World Health Assembly, 19 May 2009. Retrieved from http://www.who.int/mediacentre/events/2009/wha62/secretary_general_speech_20090519/en

Béné, C., Godfrey Wood, R., Newsham, A., & Davies, M. (2012). *Resilience: New utopia or new tyranny? Reflection about the potentials and limits of the concept of resilience in relation to vulnerability reduction programmes* (IDS Working Paper 405, September 2012). Brighton: IDS. Retrieved from http://www.ids.ac.uk/publication/resilience-new-utopia-or-new-tyranny

Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: MIT Press.

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. Cambridge, MA: MIT Press.

Bourbeau, P. (2013). Resiliencism: Premises and promises in securitisation research. *Resilience: International Policies, Practices and Discourses*, *1*(1), 3-17.

Bourbeau, P. (2015a). Resiliencism and security studies: Initiating a dialogue. In T. Balzacq (Ed.), *Contesting security* (pp. 173-188). Abingdon: Routledge.

Bourbeau, P. (2015b). Resilience and international politics: Premises, debates, agenda. *International Studies Review*, forthcoming.

Braybrooke, D, & Lindblom, C. E. (1963). *A strategy of decision: Policy evaluation as a social process.* New York, NY: Free Press.

Čas, J., Strauss, S, Amicelle, A., Ball, K., Hallinan, D., Friedewald, M., & Szekely, I. (2015). Social and economic costs of surveillance. In D. Wright & R. Kreissl (Eds.), *Surveillance in Europe* (pp. 211-258). London: Routledge.

Chandler, D. (2012). Resilience and human security: The post-interventionist paradigm. *Security Dialogue*, *43*(3), 213-229.

Chandler, D. (2013a). Editorial. *Resilience: International Policies, Practices and Discourses*, *1(1),* 1.

Chandler, D. (2013b). Pre-emptive strike: A response to "resisting resilience". *Radical Philosophy*, *179*, 58-59.

Chandler, D. (2015). Resilience and the "everyday": Beyond the paradox of "liberal peace". *Review of International Studies*, *41*(1), 27-48.

Cho, A., Willis, S., & Stewart-Weeks, M. (2011). *The resilient society: innovation, productivity, and the art and practice of connectedness*. San José, CA: Cisco Internet Business Solutions Group (IBSG). Retrieved from http://www.cisco.com/web/about/ac79/docs/ps/The-Resilient-Society_IBSG.pdf

Clarke, R. (2013). Notes of 5 February 2013 for the Advisory Board of the Increasing Resilience in Surveillance Societies (IRISS) project. Retrieved from http://www.rogerclarke.com/DV/IRISSR.html

Conway, G., Waage, J. K., & Delaney, S. (2010). *Science and innovation for development.* London: UK Collaborative on Development Science.

Demerath, N. J. III, & Peterson, R. A. (Eds.). (1967). *System, change and conflict: A reader on contemporary sociological theory and the debate over functionalism*. New York, NY: Free Press.

Deutsch, K. W. (1963). *The nerves of government: Models of political communication and control*. New York, NY: Free Press of Glencoe.

Durkheim, E. (1984 [1893]). *The division of labor in society*. New York, NY: Free Press/Macmillan.

Easton, D. (1965). *A systems analysis of political life*. New York, NY: John Wiley & Sons.

Emery, F. E. (Ed.). (1969). *Systems thinking: Selected readings*. Harmondsworth: Penguin Books.

European Commission. (2012). *Communication from the Commission to the European Parliament and the Council—The EU approach to resilience: Learning from food security crises* (COM(2012) 586 Final, Brussels, 3.10.2012). Brussels: European Commission.

Evans, B., & Reid, J. (2013). Dangerously exposed: The life and death of the resilient subject. *Resilience: International Policies, Practices and Discourses*, *1*(2), 83-98.

Feibleman, J., & Friend, J. W. (1945). The structure and function of organization. *The Philosophical Review*, *54*(1), 19-44.

Fernandez, L. A., & Huey, L. (2009). Is resistance futile? Thoughts on resisting surveillance. *Surveillance and Society*, *6*(3), 199-202.

Folke, C. (2006). Resilience: The emergence of a perspective for social-ecological systems analysis. *Global Environmental Change*, *16*, 253-267.

Ford, R. (2004, August 16). Beware rise of Big Brother state, warns data watchdog, *The Times*.

Greenwald, G. (2014). *No place to hide*. London: Hamish Hamilton.

Hall, P., & Lamont, M. (Eds.). (2013a). *Social resilience in the neoliberal era*. Cambridge: Cambridge University Press.

Hall, P., & Lamont, M. (2013b). Introduction. In P. Hall & M. Lamont (Eds.), *Social resilience in the neoliberal era*. Cambridge: Cambridge University Press.

Hamel, G., & Välikangas, L. (2003). The quest for resilience. *Harvard Business Review*, 1 September, Watertown, MA: Harvard Business Publishing. Retrieved from https://hbr.org/2003/09/the-quest-for-resilience

Holling, C. S. (1998). Two cultures of ecology. *Conservation Ecology*, *2*(2), article 4. Retrieved from http://www.consecol.org/vol2/iss2/art4

Hood, C. C. (1983). *The Tools of government*. London: Macmillan.

International Strategy for Disaster Reduction (ISDR).

(2004). *Living with risk: A global review of disaster reduction initiatives* (Volume I). New York and Geneva: United Nations. Retrieved from http://www.unisdr.org/files/657_lwr1.pdf

Introna, L., & Gibbons, A. (2009). Networks and resistance: Investigating online advocacy networks as a modality for resisting state surveillance. *Surveillance and Society*, *6*(3), 233-258.

Loader, I., & Walker, N. (2007). *Civilizing security.* Cambridge: Cambridge University Press.

Longstaff, P. H. (2005). *Security, resilience, and communication in unpredictable environments such as terrorism, natural disasters and complex technology.* Cambridge, MA: Center for Information Policy Research, Harvard University. Retrieved from http://pirp.harvard.edu/pubs_pdf/longsta/ longsta-p05-3.pdf

Los, M. (2002). Post-communist fear of crime and the commercialization of security. *Theoretical Criminology*, *6*(2), 165-188.

Luthar, S. S., Cicchetti, D., & Becker, B. (2000). The construct of resilience: A critical evaluation and guidelines for future work. *Child Development*, *71*(3), 543-562.

Lyon, D. (Ed.). (2003a). *Surveillance as social sorting: Privacy, risk and digital discrimination.* London: Routledge.

Lyon, D. (2003b). *Surveillance after September 1.* Cambridge: Polity Press.

Martin, A., Brakel, R. van, & Bernhard, D. (2009). Understanding resistance to digital surveillance: Towards a multidisciplinary, multi-actor framework. *Surveillance and Society*, *6*(3), 213-232.

Marx, G. T. (1987). Restoring realism and logic to the covert facilitation debate. *Journal of Social Issues*, *43*(3), 43-55.

Marx, G. T. (2015). Security and surveillance contests: Resistance and counter-resistance. In T. Balzacq (Ed.), *Contesting security* (pp. 15-28). Abingdon: Routledge.

Neocleous, M. (2013a). Resisting resilience. *Radical Philosophy*, *178*, 2-7.

Neocleous, M. (2013b). A reply. *Radical Philosophy*, *179*, 59.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press.

Parsons, T. (1951). *The social system*. New York, NY: Free Press of Glencoe.

Putnam, R. D. (2000). *Bowling alone: the collapse and revival of American community*. New York, NY: Simon & Schuster.

Raab, C. D. (2012). Privacy, social values and the public interest. In A. Busch & J. Hofmann (Eds.), *Politik und die Regulierung von Information [Politics and the Regulation of Information], Politische Vierteljahresschrift Sonderheft 46* (pp. 129-151). Baden-Baden: Nomos Verlagsgesellschaft.

Raab, C. D. (2014). Privacy as a security value. In D. W. Schartum, L. Bygrave, & A. G. B. Bekken (Eds.), *Jon Bing: En Hyllest/A Tribute* (pp. 39-58). Oslo: Gyldendal.

Raab, C., Hallinan, D., Amicelle, A., Galdon Clavell, G., Galetta, A., De Hert, P., & Jones, R. (2015). Effects of surveillance on civil liberties and fundamental rights in Europe. In D. Wright & R. Kreissl (Eds.), *Surveillance in Europe* (pp. 259-318). London: Routledge.

Sampson, R. J. (2008). Collective efficacy theory: Lessons learned and directions for future inquiry. In F. Cullen, J. Wright, & K. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 149-167). New Brunswick: Transaction Publishers.

Sanchez, A. (2009). Facebook feeding frenzy: Resistance-through-distance and resistance-through-persistence in the societied network. *Surveillance and Society*, *6*(3), 275-293.

Slater, T. (2014, January 28). The resilience of neoliberal urbanism, *Open Security*. Retrieved from http://www.opendemocracy.net/opensecurity/tom-slater/resilience-of-neoliberal-urbanism

Solove, D. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Szekely, I. (2008). Hungary. In J. Rule & G. Greenleaf (Eds.), *Global privacy protection: The first generation* (pp. 174-206). Cheltenham: Edward Elgar.

Taleb, N. N. (2013). *Antifragile*. London: Penguin (Allen Lane).

The Montpellier Panel (2012). *Growth with resilience: Opportunities in African agriculture*. London: Agriculture for Impact. Retrieved from https://workspace.imperial.ac.uk/africanagriculturaldevelopment/Public/Montpellier%20Panel%20Report%202012.pdf

UK Cabinet Office. (2011a). *The UK cyber security strategy protecting and promoting the UK in a digital world*. London: Cabinet Office. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

UK Cabinet Office. (2011b). *Strategic national framework on community resilience*. London: UK Cabinet Office. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60922/Strategic-National-Framework-on-Community-Resilience_0.pdf

UK Cabinet Office. (2013). *Resilience in society: Infrastructure, communities and businesses—How networks and individuals can support the country's emergency planning, response and recovery, and keep systems and services running*. London: UK Cabinet Office. Retrieved from https://www.gov.uk/resilience-in-society-infrastructure-communities-and-businesses

UK Home Office. (2011). *CONTEST: The United Kingdom's strategy for countering terrorism* (Cm 8123).

London: The Stationery Office Limited.

UN Commission on Narcotic Drugs/Commission on Crime Prevention and Criminal Justice. (2010). Drug control, crime prevention and criminal justice: A Human Rights perspective (Note by the Executive Director), E/CN.7/2010/CRP.6–E/CN.15/2010/CRP.1, 3 March 2010. Retrieved from http://www.unodc.org/documents/commissions/CND-Uploads/CND-53 RelatedFiles/ECN72010_CRP6eV1051605.pdf

UN Security Council, Counter-Terrorism Committee (CTED). (2013). Special Event, 24 May 2013. Retrieved from http://www.un.org/en/sc/ctc/news/2013-05-30_Special_Event_New_Tech.html and http://www.un.org/en/sc/ctc/docs/2013/2013-05-24_opening_stmt_chair.pdf

UN System Task Team on the Post-2015 UN Development Agenda. (2012). *Disaster risk and resilience—Thematic Think Piece*, May 2012. Retrieved from http://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/3_disaster_risk_resilience.pdf

United Nations Secretary-General's High-level Panel on Global Sustainability. (2012). *Resilient people, resilient planet: A future worth choosing*. New York, NY: United Nations. Retrieved from https://en.unesco.org/system/files/GSP_Report_web_final.pdf

Walker, B., & Salt, D. (2006). *Resilience thinking: Sustaining ecosystems and people in a changing world*. Washington, DC: Island Press.

Walklate, S., & Mythen, G. (2015). *Contradictions of terrorism: Security, risk and resilience*. Abingdon: Routledge.

Wells, H., & Wills, D. (2009). Individualism and identity: Resistance to speed cameras in the UK. *Surveillance and Society*, *6*(3), 259-274.

White, I., & O'Hare, P. (2014). From rhetoric to reality: Which resilience, why resilience, and whose resilience in spatial planning? *Environment and Planning C: Government and Policy*, *32*(5), 934-950.

Wiener, N. (1954). *The human use of human beings: Cybernetics and society*. Garden City, NY: Doubleday Anchor Books.

Wright, D., & Kreissl, R. (2015). Resilience in Europe's surveillance society. In D. Wright & R. Kreissl (Eds.), *Surveillance in Europe* (pp. 319-359). London: Routledge.

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, *28*(3), 277-298.

Yusuf, S. (2012). *The resilience of the human rights norm in an era of counter-terrorism* (UNISCI Discussion papers no. 28, January 2012). Madrid: Research Unit on International Security and Cooperation (UNISCI). Retrieved from http://revistas.ucm.es/index.php/UNIS/article/viewFile/38472/37211

About the Authors

Charles Raab

Charles Raab is Professorial Fellow, University of Edinburgh, and a Director of the Centre for Research into Information, Surveillance and Privacy (CRISP). His research concerns privacy, surveillance, security and democracy. He has given evidence to UK parliamentary committees and was Specialist Adviser to the House of Lords Constitution Committee for the inquiry, *Surveillance: Citizens and the State*, HL Paper 18, Session 2008-09. He is a Fellow of the Academy of Social Sciences and a Fellow of the Royal Society of Arts.

Dr. Richard Jones

Richard Jones is Lecturer in Criminology and Mid-Career Research Development Fellow at the School of Law, University of Edinburgh, UK. He has a PhD in Criminology from the Institute of Criminology, University of Cambridge, and has been a Visiting Academic at the Centre for Criminology, University of Oxford. His research focuses on the use of new technologies in criminal justice and crime control. He was a member of the EU's FP7 IRISS Project on surveillance, resilience and democracy, and was an External Expert on Cybercrime for the FP7 FIDUCIA project.

Dr. Ivan Szekely

Ivan Szekely, social informatist, is an internationally known expert in the multidisciplinary fields of data protection and freedom of information. A long-time independent researcher, consultant and university lecturer, as well as former chief counsellor of the Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information, Szekely is at present Senior Research Fellow of the Open Society Archives at Central European University, associate professor at the Budapest University of Technology and Economics, and advisory board member of the Eotvos Karoly Policy Institute.

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 42-52
Doi: 10.17645/mac.v3i2.270

Article

The Copyright Surveillance Industry

Mike Zajko

Department of Sociology, University of Alberta, Edmonton, T6G 2H4, Canada; E-Mail: zajko@ualberta

Submitted: 9 April 2015 | In Revised Form: 20 June 2015 | Accepted: 13 July 2015 |
Published: 30 September 2015

Abstract

Creative works are now increasingly distributed as digital “content” through the internet, and copyright law has created powerful incentives to monitor and control these flows. This paper analyzes the surveillance industry that has emerged as a result. Copyright surveillance systems identify copyright infringement online and identify persons to hold responsible for infringing acts. These practices have raised fundamental questions about the nature of identification and attribution on the internet, as well as the increasing use of algorithms to make legal distinctions. New technologies have threatened the profits of some media industries through copyright infringement, but also enabled profitable forms of mass copyright surveillance and enforcement. Rather than a system of perfect control, copyright enforcement continues to be selective and uneven, but its broad reach results in systemic harm and provides opportunities for exploitation. It is only by scrutinizing copyright surveillance practices and copyright enforcement measures that we can evaluate these consequences.

Keywords

algorithmic; copyright surveillance; copyright enforcement; identification; internet

Issue

This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction

Much of our daily lives now involve interacting with digital “content”. The relationships we have with these digital goods are governed in part by intellectual property rights, and a new industry has developed to take advantage of this legal fact. The copyright surveillance industry monitors the distribution and use of copyrighted works, identifies instances of copyright infringement, and responds against allegedly infringing uses and individuals. Dedicated companies use automated methods to operate at enormous scale, scanning millions of hours of audio and video each day, and bringing suit against hundreds of thousands of individuals each year. The questions I am posing are: how are the data packets and digital fragments passing through our computer networks identified as copyrighted content? How are these digital flows traced to identifiable individuals, and how are persons held responsible for internet traffic? What are the consequences of these determinations for data flows as well as people?

In short then, my research questions are about identification based on digital traces. One set deals with identifying traffic flows and content as intellectual property, the second set deals with identifying people and holding them accountable for traffic flows. Traffic and content are identified through algorithmic comparisons to known “signatures” or characteristics. Individuals can be identified by comparing numeric identifiers (IP addresses) recorded by monitoring software to logs maintained by internet service providers. Both methods can result in misidentification and reduce the complexities of copyright law to opaque decisions made by automated systems. My paper concludes by analyzing copyright trolling, a specific kind of surveillance and enforcement that combines the two forms of identification (of content and persons) in a particularly exploitative manner. I argue that systemic harms result from today's wide-ranging copyright regimes, although copyright's enforcement remains contingent and uneven. The internet has been seen as a threat to copyright, but copyright surveillance and enforcement technologies have also come a long way in the internet era, and are now the tools of a profitable industry.

Copyright is a convoluted body of law with strange consequences for a digitally-networked society. It justifies constraints on our behavior, but is also routinely violated as we go about our daily lives (Greenberg, 2014, pp. 82-83). Copyright allows people and institutions to claim a monopoly in the use of a piece of writing, or an image, or the tiniest fragment of recorded sound. It enforces scarcity by restricting copying—an act that is essential to human creativity (Cohen, 2012, ch. 4) and also what our computers and networks are designed to do best. Because of this, digital networks have threatened copyright, but they also allow for pervasive forms of copyright surveillance and enforcement that have become the business model of a dedicated industry. The sweeping scope of this industry has disrupted the traditional "equilibrium" of copyright's under-enforcement (Balganesh, 2013b; Lessig, 2001, pp. 249-250). Copyright can now be enforced against persons and actions that would have previously escaped copyright owners' attention, but this enforcement is uneven and inconsistent. Rather than seeking total control over the distribution of creative works, copyright enforcement is selective, tolerating some uses and intervening against others. This is because copyright depends on private actors bringing forward claims of infringement, and the pursuit of such claims is not always advantageous or desirable. On the other hand, some of the actors described below have built businesses dedicated to pursuing "profit-based litigation" (DeBriyn, 2012) and demanding monetary settlements from scores of alleged infringers.

Copyright surveillance is an international business, and the copyright enforcement actions that follow an identification of infringement are often carried out without state involvement. But state-backed legal regimes remain in the background, with their threats of liability and sovereign violence. The internet sometimes still seems like a lawless place that frustrates state controls, but it consists of physical networks based in territories and jurisdictions. It is these networks' territorial basis that allows the state-backed monopolies of copyright to have any meaningful effect. This also makes copyright and the industries it supports vulnerable to legal and political reforms.

2. Surveilling Digital Flows for Intellectual Property

Much of the data circulating through our networks can be claimed as the intellectual property of some person or legal entity. Any unauthorized use or reproduction of this data can therefore be a violation of "intellectual property rights". The rightsholders of this digital content are often part of massive industries (most notably the music and film industries) that have turned their attention to the internet since the 1990s. As a consequence, a new industry has developed to offer copyright surveillance and enforcement as a service. This is an industry that depends on the fact of infringement to support its existence (Lobato & Thomas, 2013), even as it ostensibly fights to stop it.

Copyright was originally developed to regulate publishers and booksellers dealing in unauthorized copies, but today all of our computers make and circulate copies of cultural goods. Before home computers and the internet, a great deal of copying and circulation also took place on a regular basis. People made photocopies, VHS and cassette recordings, sang popular lyrics, and repurposed melodies. But this behavior largely escaped the notice of copyright owners. It was ephemeral, dispersed, impossible to track and difficult to control. The internet is different. Its traffic is visible by default, and content can be accessed around the world. The amount of internet traffic that arguably infringes copyright has become so large that human intervention cannot possibly keep up with it.

Fortunately for copyright owners, we now live in an age of algorithmic surveillance and algorithmic enforcement (Depoorter & Walker, 2013, pp. 333-335). Because algorithms are poor at adjudicating the intricacies of copyright law, these systems regularly generate false positives (see Depoorter & Walker, 2013, p. 335; Katyal, 2009, pp. 414-415). But they are effective enough to serve the interests of copyright owners, and are having a massive effect on the availability of online content. Algorithmically-selected links are now hauled off the web by the million, and with the assistance of internet service providers (ISPs), thousands of allegedly infringing individuals can be identified and threatened by the agents of copyright owners (copyright surveillance companies and law firms).

Below, I outline the global scale of the copyright surveillance and enforcement industry and analyze some of its common practices. This analysis is furthered by internal emails and documents from MediaDefender—once one of the industry's most notable companies. While MediaDefender surveilled peer-to-peer networks, algorithmic copyright surveillance and enforcement is increasingly built-in to internet services, with YouTube's Content ID system being the most notable example. My paper discusses the case of a video caught by Content ID's extra-judicial copyright enforcement system, before closing with a more recent trend, in which BitTorrent surveillance services have been used to drive profit-seeking copyright lawsuits in several countries. But first, I relate my interest in identification and data flows to previous work in the fields of internet and surveillance studies, where social theory has taken different approaches to related problems.

3. Digital Identification and Social Theory

Surveillance scholars have long been interested in what Clarke (1988) called "dataveillance": the surveillance of data generated by persons, and the tracking of persons through data (see Elmer, 2004, pp. 36-39). In one influential contribution to surveillance studies, Haggerty and Eriscson (2000, pp. 611-614) discuss how persons and their bodies are transformed into data, generating so-called "data doubles" that are then used as the basis of discriminations among populations. But a great deal of copyright surveillance is not interested in monitoring persons or populations. In these cases, the targets of surveillance and intervention are traffic flows—not people. Surveillance companies and their monitoring algorithms are often unconcerned about the identities of the persons that can be linked to, or held responsible for this traffic. The goal is to discriminate among content and act against anything identified as infringement, rather than against the infringing party.

The consequences of this kind of copyright enforcement are not limited to some separate realm of data or "pure virtuality" (Haggerty & Ericson, 2000, p. 611). While the distinction between online and offline, or digital and physical can still have its uses, it is the problematic link between them that deserves more focus. Increasingly, the trend in social theory has been away from "digital dualism" (particularly the dichotomy of "real" and "virtual") and towards an appreciation of how our reality is constituted through digital technologies and embodied experience, or the relationship between bodies and code (Jurgenson, 2012; Wellman & Haythornthwaite, 2002). YouTube videos do not reside and circulate in cyberspace. They are part of our world, and when a video is blocked there can be very real and material consequences for the persons involved (as seen in the Lansdowne Library case discussed below).

The other kind of copyright surveillance discussed herein does indeed target people through data, but approaches its problem from the opposite direction typically of interest to surveillance studies. Rather than "abstracting human bodies from their territorial settings and separating them into a series of discrete flows" (Haggerty & Ericson, 2000, p. 606), the process I am interested in here is how these digital flows are attributed to human bodies, or how people can be identified by "suturing or coupling of pieces of information in disjunctive time and scattered spaces" (Monahan, 2009, p. 158). The specific example of this process considered herein is "copyright trolling", in which an IP address linked to file-sharing activity must be translated into a street address and a particular resident (typically, the internet subscriber). This translation cannot be achieved simply through technical means—there is no method that an outside observer can use to independently pin the IP address (used to route packets of information) to an individual residence. While copyright surveillance companies can monitor file-sharing traffic and record the IP addresses of the devices involved, they must secure the compliance of an ISP to correlate these digital addresses with subscribers' street addresses. Typically, this compliance is achieved under the weight of the law governing the territory in question.

These concerns of copyright surveillance are related to two fundamental problems of our networked age. The first problem is control over the cultural objects and the information circulating through our networks (see Poster, 2006, p. 186). In other words, how internet controls can be achieved, and to what effect. The second problem is holding individuals accountable for data traffic, or how digital records can be sutured together to identify a person "behind" the internet traffic (see Poster, 2006, pp. 113-116). While these questions are now fundamental concerns for a variety of actors, it is important to understand how copyright surveillance and enforcement companies have taken to answering them, given the systemic harms that copyright regimes are capable of producing (see Cohen, 2012, ch. 4).

4. Copyright Surveillance at a Glance

As described above, copyright surveillance has two basic targets: content and persons (see Table 1 below). The vast majority of copyright surveillance does not aim to identify infringing individuals. Instead, algorithmic surveillance is used on a massive scale to identify copyrighted content by comparing digital fragments to particular "signatures". This involves systematically monitoring file-sharing protocols or "crawling" websites. The algorithms tasked with this surveillance look for certain file names or other characteristics of the content being distributed online, and compare these to a database of known copyrighted content. What happens when the algorithm detects potential infringement depends on the party conducting the surveillance (or more likely, the party paying for it as a service). Assuming that this party is a copyright owner, they may do nothing at all. Knowing what is being downloaded or shared across the internet can be useful information. Companies that provide copyright surveillance often promote their services as a way to gather market information or "business intelligence" (Lobato & Thomas, 2013). However, my main interest is copyright surveillance that is geared toward intervention. This can include having the content removed, making it more difficult to access, or targeting the persons allegedly infringing copyright. Individuals can be targeted for lawsuits, or be subject to private enforcement regimes like the US Copyright Alert System (Zimmerman, 2014), which (like Canada's "notice-and-notice" system, see Tarantino, 2012) notifies internet subscribers when their IP address has been linked to infringing activity.

Table 1. Two basic types of copyright surveillance and associated enforcement.

Target	Means of Identification	Possible Interventions	Examples
Content	Comparing file properties to a known signature	Takedown notices, automated filtering, traffic disruption	DMCA takedowns, YouTube Content ID, file interdiction (MediaDefender)
Persons	Recording IP addresses and reconciling these with an ISP's logs	Deterrent/educational notices, degraded internet service, lawsuits	HADOPI, Canadian notice-and-notice, US Copyright Alert System, RIAA file-sharing lawsuits, copyright trolling

Copyright surveillance is almost entirely the domain of private industry. While the French internet copyright regime (HADOPI) created a government agency dedicated to enforcement, the system relies on a private company to monitor the country's internet traffic (see Bridy, 2011, pp. 733-735). The copyright surveillance industry is modest in size (a large monitoring and enforcement company might have a few dozen employees), but it monitors an enormous scope of online activity and facilitates sweeping legal interventions. Some copyright owners employ small surveillance and enforcement firms and achieve massive reach by leveraging algorithmic methods (Farivar, 2012). Monitoring the public or quasi-public internet for copyrighted content can in theory be achieved at scale by anyone, including academics (Chothia, Cova, Novakovic, & Toro, 2013; Zhang, Dhungel, Wu, & Ross, 2011). Copyright surveillance companies do use specialized software, but they generally do not enjoy any privileged access to internet traffic.

The first of these copyright surveillance companies were founded in 1999 and 2000, during the rapid rise of the file-sharing service Napster (Doan, 2000) and the accompanying legal campaign to stop internet piracy. For several years this campaign by the music industry generated lawsuits against tens of thousands of US individuals accused of online infringement. Over the course of the mid to late 2000s these efforts were largely abandoned. Today they can be recognized as a failed attempt to criminalize widespread and normalized behavior (Bachmann & Jaishankar, 2011; Harris, 2012). However, copyright surveillance has continued towards other ends, such as targeting web services and search engines. In recent years, mass file-sharing lawsuits have resurfaced, but these have generally been oriented towards generating revenue for minor copyright owners rather than deterring infringement of major creative works.

Deeper insight into the copyright surveillance industry was made possible in 2007, when six months of internal files and emails from US-based MediaDefender appeared online (see Roth, 2008; Zetter, 2007). At the time of this supposed hack of the company, MediaDefender was one of the more notable firms in the industry, having been purchased for $43 million in 2005 (Mennecke, 2005). The company was working to expand into a number of business opportunities, including helping to identify individuals sharing child pornography, and its own video download service. However, the majority of MediaDefender's business activity involved "protecting" particular titles for copyright owners by monitoring several file-sharing networks for newly released or soon-to-be released titles. When these files were found, downloads could be disrupted through various means. These included flooding file-sharing networks with "decoy" or "spoof" versions (which appear genuine, but are instead unplayable, limited to promotional content, or redirect to an approved source. See Anderson, 2007; Katyal, 2003, pp. 356-358).

MediaDefender did not generally collect evidence or IP addresses for use in litigation, but it did record and share data on file-sharing for other purposes. These included answering queries from copyright owners about the amount of file-sharing in a particular country or region. In two e-mail exchanges, rightsholders asked the company about the popularity of individual songs being considered for release as singles. MediaDefender's clients included some of the world's biggest copyright owners (Universal, Paramount, Sony BMG). One "small monitoring contract" with a major record label paid $10,000 a month to monitor three file sharing networks for the presence of particular files. Different levels of protection, for different lengths of time, were offered for between $5,000 and $15,000 per title (Anderson, 2007). In one email exchange during 2007, it was estimated that the company of approximately 60 employees was working on around 3,000 projects at once, with company servers pushing out around 3 billion decoy and spoof files a day.

MediaDefender's fortunes declined following the compromise of its files in 2007, and the company eventually went out of business. But the information disclosed about its operations can still tell us several things. First, even a small firm can monitor and intervene against file sharing on a massive scale. MediaDefender's methodology combined algorithmic discrimination with human judgment, but it was the algorithms that enabled its broad scope. The following section elaborates on how this algorithmic copyright enforcement has evolved since MediaDefender's heyday, through built-in systems such as YouTube's Content ID. Afterwards, I will turn to the topic of copyright surveillance for the purposes of personal identification.

5. Caught in the YouTube Vortex

In 2012 the Lansdowne Public Library and its Teen Advisory Board in Pennsylvania made a video promoting reading and uploaded it to YouTube. The video parodied Michael Jackson's "Beat It" (Read It, 2012), featuring teens dancing and singing about reading. In less than three days the video was identified as potentially infringing copyright and taken down from YouTube. In their efforts to restore the video over the following year, library staff would need to navigate the tangles of copyright law, content ownership, and algorithmic enforcement.

It was unclear who had been responsible for the takedown in the first place, since YouTube's takedown system is automated, but operates under the direction of copyright owners. The system initially referred the library to Warner/Chappell Music (Mengers, 2013), but Jackson's music has been transferred to Sony/ATV. The librarian who had filmed the video filled out the forms to appeal the decision and sought licensing from Sony (Schwartz, 2012). She also made personal appeals to Sony, which included travelling to New York and trying to enter Sony's offices. At one point, Sony claimed that they wanted the lyrics in the video changed. Later the company allowed to video to be put online, but only on the library's website and not on any other site, and only for a limited time period (Mengers, 2012). After national news media began covering the story, Sony moved to allow the video to be re-instated (Schwartz, 2012).

Was the video infringing? Was it fair use (see Schwartz, 2012)? Because of the legal uncertainties and gray areas of copyright law, these legal distinctions can only be made by a court (see Katyal, 2009, pp. 411-412; Lee, 2008). But the absence of a court's judgment did not prevent an algorithmic judgment. Months later, the same YouTube video had its audio muted through an automated enforcement action. Once again, an algorithm had been tripped, silencing the library and its teens. Sony denied being behind the muting. According to the Library's director, Sony claimed that they did not have the power to restore the audio, and that the content had been caught in the "YouTube vortex" (New Media Rights, 2013). The library phoned YouTube but could not speak to a human being (Mengers, 2013). One of the librarians eventually submitted a claim through YouTube's online appeal process, but she needed the help of a lawyer to craft a fair use argument which would be effective in having the audio restored (Mengers, 2013; New Media Rights, 2013). What eventually turned out to be a copyright success story required exceptional efforts on the part of library staff, as well as legal help to properly engage with YouTube's enforcement regime and appeal its algorithms.

6. Scan and Notice

Online copyright enforcement is generally meant to deny or restrict the availability of content. Denial can be achieved either by directly disrupting access (as in MediaDefender's interdiction efforts), through built-in enforcement regimes such as YouTube's (see below), or by using existing copyright laws to issue what are known as "takedown notices" for content (Lobato & Thomas, 2013, p. 615). Millions of pieces of content are targeted by such notices every week, which can be effective wherever ISPs and online services are required to take them seriously. The processing of takedown notices is crucial for these companies to maintain "safe harbor" protection under the copyright laws of the US, EU, and Canada (among other nations, see Fernández-Díez, 2014; Tarantino, 2012). Safe harbor protects companies providing internet services against liability for infringement carried out by their users. However, this protection often only applies to companies as long as they remain unaware that their users are infringing copyright (Fernández-Díez, 2014, pp. 67-69). Under safe harbor, service providers have an incentive to limit what they know about their users' activities. When a legitimate takedown notice arrives informing them of infringement on their service, service providers are obliged to take action.

As a consequence, copyright surveillance companies have been algorithmically flagging infringement across the web and sending a growing deluge of notices to major content hosting platforms. Online service providers have to decide whether each notice is legitimate and should be complied with. Google processed a weekly average of between seven and nine million URLs in late 2014 (Google, 2015), with each request from a major copyright owner typically listing thousands of URLs for removal. Just as the employees of copyright surveillance companies use automated scanning and algorithmic discrimination to create these lists, Google uses its proprietary blend of algorithms and human review to decide which takedown notices should be complied with, and which should be rejected (Google rejected less than 1% of these notices in 2013, see Google, 2014, p. 13).

YouTube (owned by Google) maintains a similar system for handling takedown notices, but also operates its own automated system for identifying infringing content, known as Content ID. This proactive system of identifying infringement was developed while YouTube was embroiled in a billion-dollar lawsuit with Viacom (which accused YouTube of not taking action against videos that it knew were infringing, see Zimmerman, 2014, pp. 264-265). Rightsholders provide YouTube with "reference files" of their content, and the site scans each uploaded video looking for a match. If Content ID matches an uploaded video to one of its 25 million or so active reference files, the copyright owner can choose to block the video (or mute its audio), show ads, or track its viewership (Google, 2014).

The algorithms behind Content ID have been refined over the years, and its appeals process has been elaborated and extended (La Rosa, 2014; Zimmerman, 2014, p. 272). Still, Content ID's proactive orientation exceeds the requirements of US law, and Google announced that in implementing it the company "goes above and beyond [its] legal responsibilities" (King, 2007). Google has created an extensive copyright monitoring and enforcement system that operates without court involvement, in part to keep the company from facing another massive lawsuit by rightsholders. In its effort to proactively police copyright, YouTube processes a staggering amount of video through Content ID (Google, 2014), and the system has helped channel over a billion dollars in advertising revenue to copyright owners (La Rosa, 2014). But those caught on the wrong side of YouTube's judgments, as in the Lansdowne Library case (see also Tarantino, 2012) have had to suffer the costs, without the transparency and due process that a court could provide (Zimmerman, 2014, p. 273).

Built-in monitoring and copyright enforcement systems are increasingly the norm for popular media-sharing websites (La Rosa, 2014). With growing numbers of people creating and distributing content online (Poster, 2006, pp. 244-249), these private copyright enforcement regimes are having a major effect in controlling the distribution of cultural goods. Algorithmic judgments may not carry the same weight as court orders, but they are effectively the law of these digital domains (see Lessig, 2006). However, some companies have combined the use of algorithmic surveillance and discrimination with the enforcement powers of the courts. They do so in order to link identifications of copyright infringement to individual persons. An entire business model has developed in recent years around identifying individuals tied to copyright infringement and compelling them to pay large penalties. The result, known as copyright trolling, might be the most exploitative use of copyright enforcement in the digitally-networked era.

7. Lawsuits and BitTorrent Trolls

Identifying persons is a relatively minor concern for the type of copyright surveillance described earlier: what matters is whether internet traffic includes copyrighted content, and whether it can be controlled. However, in the early 2000s many major US copyright owners felt they could achieve control through deterrence—by identifying and suing thousands of individuals accused of sharing songs. Their efforts failed (DeBriyn, 2012, pp. 84–85), and for a time copyright owners' lawsuits shifted from individuals to institutions (like YouTube and The Pirate Bay) that allegedly facilitated infringement. But by 2010, a new approach took hold among some of the more marginal copyright owners and their lawyers. Courts once again saw thousands of persons targeted in infringement suits, and judges were asked to help identify these defendants on the basis of IP addresses.

The actors bringing these sorts of suits are often described as "copyright trolls", but there are disagreements about just what distinguishes a troll from a more legitimate plaintiff. Trolling operations vary and are legally opportunistic, and it has proven difficult to define copyright trolls in a way that captures more than a portion of such operations (see Sag, 2015). Because of this, I avoid labeling any specific companies as copyright trolls. Instead (and largely in agreement with Sag, 2015), I refer to copyright trolling as a practice—one that threatens large numbers of individuals with copyright infringement claims, with the primary goal of profiting from settlements (or default judgments) rather than proceeding to trial on the merits of a case (see Curran, 2013).

While major copyright owners can engage in trolling, they generally prefer not to. This is typically the domain of smaller companies that do not receive large profits through sales and licensing, and see settlements as an easy way of generating revenue from individuals who are not paying for their works. Trolling is "profit-based litigation" (DeBriyn, 2012, p. 86), and to be successful it depends on accused infringers fearing the price of statutory damages and settling for smaller amounts. In the large subset of copyright trolling cases dealing with pornography, the pressure on defendants can be amplified by the fear of being publicly associated with pornography titles (Curran, 2013).

Copyright trolling is a strategy that depends on linking internet traffic to particular individuals, which is where copyright surveillance companies come into play. These companies monitor online traffic, record the IP addresses involved in sharing certain files, and hand the list to a law firm. The law firm then undertakes the next step by approaching the ISP that assigned the IP addresses, and having the ISP consult its logs to determine which address was assigned to which subscriber at a given time. Frequently, this requires a court to compel the ISP to disclose the subscriber's information (Anderson, 2010). The copyright surveillance company does not enter into the process again unless the plaintiff is forced to further substantiate the claim of infringement before a court.

Copyright trolling (sometimes called "speculative invoicing") is often thought of as a particularly American practice, since statutory damages in the US can be up to $150,000 per work infringed, and the average cost of defending a copyright infringement case through trial (excluding judgment and awards) ranges between $384,000 and $2 million, depending on the size of the copyright claim (Am. Intellectual Law Ass'n, of the Economic Prop. Report Survey 2011, cited in Balganesh, 2013a, p. 2280; Depoorter & Walker, 2013). This makes settling for between $1500 and $5000 a more attractive option, which has led many commentators to liken the process to extortion or "legal ransom" (Curran, 2013). However, the legal strategy of copyright trolling has also seen extensive use in the UK (*Golden Eye [International] Ltd. & Anor v Telefonica UK Ltd*., 2012) and may have been pioneered in Germany (Lobato & Thomas, 2013, p. 618; Roettgers, 2011). In 2010, tens of thousands of individuals had been sued in this manner in the US (Anderson, 2010). By 2011 the number exceeded 200,000 (Ernesto, 2011) and was possibly much higher in Germany (Roettgers, 2011). By 2014, copyright trolling cases made up the majority of copyright cases filed in several US federal court districts (Sag, 2015). No one knows just how many individuals have settled in these cases or how much money has been collected in total, although millions of dollars have clearly been paid to different trolling operations.

While some trolling operations have specialized in the copying of images, news articles, and audio samples (Curran, 2013; Polonsky, 2012), my focus is on trolling cases that target file-sharing on BitTorrent. The BitTorrent protocol rose to popularity in the mid-2000s as a way of distributing and sharing large files, which made it ideal for videos. Since this protocol operates as a distributed system and has no central point of control, it cannot be shut down by court order in the same way as earlier file-sharing systems such as Napster and Kazaa. Traffic on BitTorrent is highly visible however, since each downloaded file is received as many small pieces from numerous users (all of whom constitute a "swarm"), and each of these contributors can be identified by an IP address. BitTorrent activity can be monitored through a number of means (Chothia et al., 2013), but in essence, it is by joining a swarm that one can record the IP addresses of all those who are also participating in it.

Just as the activities and IP addresses of downloaders and uploaders are largely visible on BitTorrent, so are the activities of copyright surveillance companies (Chothia et al., 2013; Ernesto, 2012). However, we know little about their methods, since these have rarely been submitted as evidence and examined in court. Copyright trolling cases, by and large, do not proceed to trial. This might be because the costs of litigating a case exceed what might be recovered as a settlement, but also because of the risk of an unfavorable judgment against the troll. The information obtained through monitoring BitTorrent is relevant primarily for the "discovery phase" of a suit, where a court order is sought to compel an ISP to identify its subscribers. With the identities of alleged infringers in hand, a troll can then proceed to demand settlements from them, and the information used to make these demands need never be assessed as evidence in a court of law. In a typical copyright trolling case, the subscriber's name and home address is all that is needed to send out a settlement letter (demanding payment of a few thousand dollars to make the suit disappear). However, depending on the plaintiff and the defendant's actions, further investigations can be carried out. In some US copyright trolling cases, defendants arguing their innocence have undertaken polygraph tests or had their computers searched by forensic examiners (Malibu Media LLC, 2014). Defendants in these cases must decide how far they are willing to go to demonstrate their innocence (versus paying the settlement), and plaintiffs must decide how far they are willing to go to pursue a settlement or judgment (houstonlawy3r, 2013).

Ultimately, the copyright troll business model depends on legal regimes and judges that can facilitate these sorts of actions. In the US, judges have by and large granted the court orders sought to identify subscribers, but legal decisions since 2013 have limited the ability of trolling cases to sweep up thousands of individuals at once (houstonlawy3r, 2013; Ren, 2013; Sag, 2015). The most egregious trolling practices have also faced the threat of legal sanctions in US courts (Haslach, 2013). In a significant UK case, a judge granted a court order to identify suspected infringers, but imposed conditions on the manner in which settlement offers could be made (*Golden Eye ([nternational] Ltd. & Anor v Telefonica UK Ltd*., 2012). Similarly, an attempt to identify thousands of subscribers in Canada was met with reservations from a judge who, citing privacy concerns and the "spectre" of the copyright troll, imposed conditions that would limit the opportunities to profit from settlement demands (*Voltage Pictures LLC v. John Doe and Jane Doe*, 2014). The case was subsequently cited to justify similar conditions in a precedent-setting Australian file-sharing suit (*Dallas Buyers Club LLC v iiNet Ltd.*, 2015).

While some of the most exploitative opportunities for trolling have been foreclosed by the above judgments, a few copyright surveillance companies have found ways to secure compliance from ISPs to identify alleged infringers without proceeding through the courts. The most notable of these has been Rightscorp, which pursues settlements for just $20, albeit on a mass scale (Mullin, 2014). In Canada, CEG-TEK has pursued somewhat larger settlements by taking advantage of the country's new copyright enforcement regime, which requires ISPs to forward notices from copyright owners to subscribers (Roberts, 2015). Just as some courts have come to oppose copyright trolling, new business models based on copyright surveillance and identification are being developed to fit changing legal environments.

8. Pervasive Surveillance, Contingent Enforcement

Widespread and vigorous copyright enforcement can be justified by the harm that infringement causes: reducing profits for artists and creative industries, thereby limiting incentives for the production of new creative works. While it is demonstrably false that every infringing act results in harm (particularly as some unauthorized uses are actively encouraged by copyright owners, see Lee, 2008), it is undeniable that forms of infringement such as file-sharing have, to some extent, been "revenue-depleting" for certain industries (Bridy, 2011, p. 711). If the aim of copyright is to lessen such harm by reducing infringement, then pervasive surveillance and severe enforcement might be legitimate approaches. If there are reasons to believe that a heavy-handed approach to copyright enforcement is counterproductive to this aim (see Bachmann & Jaishankar, 2011; Harris, 2012), then as with any form of illegality, we might debate which kinds of infringement are best addressed through which enforcement measures, or to what extent the law is being "overenforced" (Balganesh, 2013b).

It is not my objective in this paper to determine the appropriate balance between the rights of copyright owners and users, or how best to combat infringement. Instead, my interest is in the rise of the copyright surveillance industry and its consequences. Digital media and networks have made it easier than ever for individuals to copy and distribute copyrighted content, but monitoring and enforcement technologies now also have a global reach. Copyright owners previously had limited insight into how their works were used and distributed (particularly for non-commercial purposes) and little ability to control such behavior. But Content ID can scan hundreds of years of video fed into YouTube each day (Google, 2014), and similar systems are being adopted by a growing number of media-sharing platforms. With limited resources, millions of IP addresses connected through BitTorrent can be monitored (Zhang et al., 2011), and the resurgence of mass litigation against file-sharers has seen hundreds of thousands of these IP addresses brought before courts for identification. These developments have dramatically extended areas of contact between individuals and copyright owners.

A number of authors have raised the fear that copyright enforcement systems were transforming our networked society into a dystopia of total surveillance and "perfect regulation" (Lessig, 2006, pp. xiii-xv) or "perfect [law] enforcement" (Mulligan, 2008). However, while copyright enforcement systems are now widely deployed, they form an uneven regulatory patchwork that is far from perfect in its discriminations. In the cases examined above, haphazard contingencies determine whether or not enforcement measures come into effect. Content ID does not enforce all copyright equally (enforcement depends on the rightsholder), and BitTorrent trolls can choose among legal jurisdictions and ISPs when seeking court orders. Many forms of copyright surveillance are not tied to any enforcement actions at all, and copyright owners frequently tolerate unauthorized use of their works for promotional purposes (Lee, 2008).

Perfect enforcement is therefore an impossible and undesirable goal, even for many rightsholders. Instead, we see pervasive copyright surveillance and uneven, contingent enforcement. As a consequence, individuals are left uncertain about which actions will be tolerated and which will be pursued as instances of infringement (Katyal, 2009, p. 418), or what uses of copyrighted content qualify as "fair" (Katyal, 2009, pp. 411-413; Lee, 2008). False positives also occur regularly as automated systems misidentify content, or copyright owners assert illegitimate claims (Depoorter & Walker, 2013). Individuals wishing to contest these claims can be left in the position of the Lansdowne Library video producers, unsure of how or where to appeal a judgment. Those who are misidentified as infringers by copyright trolls are left weighing the price of a settlement against the costs of demonstrating their innocence in court (Balganesh, 2013a). Copyright enforcement might be inconsistent and uncertain, but those caught in its net experience significant harms.

This paper's selection of cases has been used to make three broad points. First, many kinds of mass copyright surveillance can be carried out with limited resources, and there is sufficient demand for these services to support a small, dedicated industry. Surveillance companies like MediaDefender demonstrated the vast reach of their algorithmic methods in the early 2000s, and web giants like YouTube can scale their monitoring capabilities to match the vast volumes of content passing through their servers. The second point is that these algorithmic judgments are inherently imperfect and unevenly applied, contributing to deep uncertainties in copyright enforcement. The harm caused when automated methods misidentify or overreach against infringement can be significant, as in the Lansdowne Library video, and those affected may have limited recourse. As a third point, it is important to recognize the systematic harms that result from expansive copyright enforcement regimes (Cohen, 2012, ch. 4), even when these operate within the law. The phenomenon of copyright trolling combines mass copyright surveillance and mass litigation, extracting settlements out of as many people as possible, but not submitting evidence to the scrutiny of a trial. Such efforts disrupt copyright's traditional "equilibrium" of under-enforcement (Balganesh, 2013b) by pursuing non-commercial cases of infringement which were largely outside the scope of enforcement before internet technologies facilitated both widespread sharing and mass surveillance. Therefore, while uses of internet technologies have harmed the traditional business models of some copyright owners, the systematic harms enabled by the business of copyright surveillance and enforcement also need to be acknowledged.

9. Conclusion

The commercialization of internet activity since the

1990s has entailed treating some digital flows as intellectual property, the idea being that much of the content circulating through the internet has an "owner" with exclusive rights to its distribution. The copyright surveillance and enforcement industries serve their clients by identifying copyrighted works and controlling their distribution, as well as identifying individuals allegedly engaged in infringement. Algorithmic tools are used to solve these problems at scale, so that even small monitoring firms can have massive reach. There is sufficient demand for these services to ensure that copyright surveillance and enforcement systems will continue to be developed and refined, particularly as private enforcement regimes like Content ID are adopted across a growing number of online platforms.

While copyright enforcement is driven by private actors, it depends on state authorities and credible threats of legal action to compel compliance and assistance from third parties. The legal foundation of these efforts makes them vulnerable to changing judicial attitudes, as well as political reforms to copyright regimes. Copyright trolling in particular has faced a growing backlash in recent years, with some courts limiting or imposing supervision over such operations. But innovative new ways have been developed to generate revenue from systematic copyright claims. These kinds of exploitative enforcement will remain a danger as long as digital flows can easily be attributed to individuals, and copyright regimes impose large monetary penalties for commonplace behavior.

Not all of the concerns discussed in this paper are specific to intellectual property rights. Any attempt to screen the vast volumes of data in circulation for illegality will require the use of algorithms to make legal distinctions, or ways to hold individuals accountable for digital flows. But the reason why copyright has been such a powerful driver of internet governance debates and policies is the large financial interest that media industries have in controlling the distribution of creative works. This same interest now supports a copyright surveillance industry, which in turn enables widespread copyright enforcement, along with enforcement's systemic harms. It can be argued that these harms are the price of preserving copyright in the era of digital networks, but there are now many examples of how such an approach can go too far, and reasons to wonder whether this is an appropriate justification. It is only by closely attending to the effects of copyright regimes and the practices they support that we can make an informed judgment on the best way forward. This requires not just the active interest of scholars, but also that copyright regimes (especially algorithmic and extra-judicial regimes) be open to scrutiny.

Acknowledgments

This paper benefited from the guidance of Kevin Haggerty and the opportunity to present at the 2014 Surveillance & Society conference.

Conflict of Interests

The author declares no conflict of interests

References

Anderson, N. (2007). Peer-to-peer poisoners: A tour of MediaDefender. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2007/03/mediadefender

Anderson, N. (2010). US anti-P2P law firms sue more in 2010 than RIAA ever did. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/news/2010/10/us-anti-p2p-law-firms-sue-more-in-2010-than-riaa-ever-did.ars

Bachmann, M., & Jaishankar, K. (2011). Suing the genie back in the bottle: The failed RIAA strategy to deter P2P network users. In *Cyber criminology: Exploring internet crimes and criminal behavior* (pp. 155-172). Boca Raton: CRC Press.

Balganesh, S. (2013a). Copyright infringement markets. *Columbia Law Review*, *113*, 2277-2332.

Balganesh, S. (2013b). The uneasy case against copyright trolls. *Southern California Law Review*, *86*, 723-781.

Bridy, A. (2011). Is online copyright enforcement scalable? *Vanderbilt Journal of Entertainment & Technology Law, 13*(4), 695-737.

Chothia, T., Cova, M., Novakovic, C., & Toro, C. G. (2013). The unbearable lightness of monitoring: Direct monitoring in BitTorrent. In A. D. Keromytis & R. D. Pietro (Eds.), *Security and privacy in communication networks* (Vol. 106, pp. 185-202). Heidelberg: Springer.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498-512.

Cohen, J. E. (2012). *Configuring the networked self*. New Haven, CT: Yale University Press.

Curran, L. S. (2013). Copyright trolls, defining the line between legal ransom letters and defending digital rights: Turning piracy into a business model or protecting creative from internet lawlessness? *John Marshall Review of Intellectual Property Law*, *13*, 170-644.

Dallas Buyers Club LLC v iiNet Ltd. (2015). No. 317 (FCA 2015).

DeBriyn, J. (2012). Shedding light on copyright trolls: An analysis of mass copyright litigation in the age of statutory damages. *UCLA Entertainment Law Review*, *19*(1), 79-112.

Depoorter, B., & Walker, R. K. (2013). Copyright false positives. *Notre Dame Law Review*, *89*(1), 319-360.

Doan, A. (2000). NetPD wants to be web's police department. *Forbes*. Retrieved from http://www.forbes.com/2000/05/05/mu9.html

Elmer, G. (2004). *Profiling machines: Mapping the personal information economy*. Cambridge, MA: The MIT Press.

Ernesto. (2011). 200,000 BitTorrent users sued in the United States. *TorrentFreak*. Retrieved from https://torrentfreak.com/200000-bittorrent-users-sued-in-the-united-states-110808

Ernesto. (2012). Anti-pirates caught spying on thousands of torrents. *TorrentFreak*. Retrieved from http://torrentfreak.com/anti-pirates-caught-spying-on-thousands-of-torrents-120829

Farivar, C. (2012). Microsoft outsources copyright enforcement to small Redmond company. Retrieved from http://arstechnica.com/business/2012/05/microsoft-outsources-copyright-enforcement-to-small-redmond-company

Fernández-Díez, I. G. (2014). Comparative analysis on national approaches to the liability of Internet intermediaries for infringement of copyright and related rights. *WIPO*. Retrieved from http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf

Golden Eye (International) Ltd. & Anor v Telefonica UK Ltd. (2012). 723 (Ch) (EWHC 2012).

Google. (2014). How Google fights piracy. *Google*. Retrieved from https://drive.google.com/file/d/0BwxyRPFduTN2NmdYdGdJQnFTeTA

Google. (2015). Copyright removal requests. *Google*. Retrieved from https://www.google.com/transparencyreport/removals/copyright

Greenberg, B. A. (2014). Copyright trolls and presumptively fair uses. *University of Colorado Law Review*, *85*, 53-128.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605-622.

Harris, D. P. (2012). The new prohibition: A look at the copyright wars through the lens of alcohol prohibition. *University of Tennessee Law Review*, *80*, 101-211.

Haslach, M. R. (2013). Trouble for trolling: Courts reject copyright trolling tactics. *Washington Journal of Law, Technology & Arts*, *9*(2), 93-115.

houstonlawy3r. (2013, December 6). CLF 2013, a year in review. *Federal Computer Crimes*. Retrieved from http://cyberlawy3r.wordpress.com/2013/12/06/2013-a-year-in-review

Jurgenson, N. (2012). When atoms meet bits: Social media, the mobile web and augmented revolution. *Future Internet*, *4*(1), 83-91.

Katyal, S. (2003). The new surveillance. *Case Western Law Review*, *54*(2), 297-385.

Katyal, S. (2009). Filtering, piracy surveillance, and disobedience. *Columbia Journal of Law & the Arts*, *32*(4), 401-426.

King, D. (2007). Latest Content ID tool for YouTube. *Google Blog*. Retrieved from http://googleblog.blogspot.com/2007/10/latest-content-id-tool-for-youtube.html

La Rosa, D. (2014). YouTube pays out over $1 billion through Content ID. *Videoter*. Retrieved from http://videoter.com/youtube-content-id-pay-1-billion

Lee, E. (2008). Warming up to user-generated content. *University of Illinois Law Review*, *2008*(5), 1459-1548.

Lessig, L. (2001). *The future of ideas: The fate of the commons in a connected world*. New York: Random House.

Lessig, L. (2006). *Code: And other laws of cyberspace* (2nd ed.). New York: Basic Books.

Lobato, R., & Thomas, J. (2013). The business of anti-piracy: New zones of enterprise in the copyright wars. *International Journal of Communication*, *6*, 606-625.

Malibu Media LLC. (2014). *Plaintiff's status and informational report for its cases in the Northern District of Illinois* (Malibu Media LLC v. John Doe). United States District Court for the Northern District of Illinois. Retrieved from http://www.scribd.com/doc/216662394/Gov-uscourts-ilnd-292270-17-0

Mengers, P. (2012). Lansdowne teens' video turns into standoff with Sony, Michael Jackson estate. *Delaware County Daily Times*. Retrieved from http://www.delcotimes.com/general-news/20121126/lansdowne-teens-video-turns-into-standoff-with-sony-michael-jackson-estate-with-videos

Mengers, P. (2013). Chalk up another win for Lansdowne kids; audio restored to "Read It" video. *Delaware County News Network*. Retrieved from http://www.delconewsnetwork.com/articles/2013/10/10/news_of_delaware_county/news/doc52567162b99d9565138161.txt

Mennecke, T. (2005). ArtistDirect Purchases MediaDefender. *Slyck News*. Retrieved from http://www.slyck.com/story875_ArtistDirect_Purchases_MediaDefender

Monahan, T. (2009). Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology*, *13*(2), 155-176.

Mulligan, C. M. (2008). Perfect enforcement of law: When to limit and when to use technology. *Richmond Journal of Law & Technology*, *14*(4), 1-49.

Mullin, J. (2014). You could be liable for $150k in penalties—settle instead for $20 per song. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2014/06/meet-rightscorp-the-internets-new-for-profit-copyright-cop

New Media Rights. (2013). Teens make parody video, but Sony tells them to beat it… just beat it! *New Media Rights*. Retrieved from http://www.newmediarights.org/teens_make_parody_video_sony_tells_them_beat_it%E2%80%A6_just_beat_it

Polonsky, I. (2012). You can't go home again: The righthaven cases and copyright trolling on the Internet. *Columbia Journal of Law & the Arts*, *36*(1), 71-101.

Poster, M. (2006). *Information please: Culture and politics in the age of digital machines*. Durham: Duke University Press Books.

Read It. (2012). Retrieved from https://www.youtube.com/watch?v=ZjwzcBTCxOo&

Ren, P. (2013). Fate of BitTorrent John Does: A civil procedure analysis of copyright litigation. *Hastings Law Journal*, *64*(4), 1343-1380.

Roberts, J. J. (2015). US firm runs mass copyright shakedown in Canada. *Gigaom*. Retrieved from https://gigaom.com/2015/03/06/us-firm-runs-mass-copyright-shakedown-in-canada

Roettgers, J. (2011). P2P Lawsuits gone wild. *Gigaom*. Retrieved from http://gigaom.com/2011/01/14/p2p-lawsuits-gone-wild

Roth, D. (2008). Hacking: The pirates can't be stopped. *Condé Nast Portfolio*. Retrieved from http://www.danielroth.net/archive/2008/01/hacking-the-pir.html

Sag, M. (2015). Copyright trolling, an empirical study. *Iowa Law Review*, *100,* 1105-1147.

Schwartz, M. (2012). Posting a parody video? Read this first. *Library Journal*. Retrieved from http://lj.libraryjournal.com/2012/11/copyright/posting-a-parody-video-read-this-first

Tarantino, B. (2012). Online infringement: Canadian "notice and notice" vs US "notice and takedown." *Entertainment & Media Law Signal*. Retrieved from http://www.entertainmentmedialawsignal.com/online-infringement-canadian-notice-and-notice-vs-us-notice-and-takedown

Voltage Pictures LLC v. John Doe and Jane Doe. (2014). No. T-2058-12 (FC 2014).

Wellman, B., & Haythornthwaite, C. (2002). Introduction. In *The Internet in everyday life* (pp. 3-41). Malden: Blackwell.

Zetter, K. (2007). Hackers smack anti-piracy firm MediaDefender again and again. *Wired*. Retrieved from http://www.wired.com/politics/security/news/2007/09/mediadefender

Zhang, C., Dhungel, P., Wu, D., & Ross, K. W. (2011). Unraveling the BitTorrent ecosystem. *IEEE Transactions on Parallel and Distributed System*, *22*(7), 1164-1177.

Zimmerman, D. L. (2014). Copyright and social media: A tale of legislative abdication. *Pace Law Review, 35*(1), 260-285.

About the Author

Mike Zajko

Mike Zajko is a PhD Candidate in the Department of Sociology at the University of Alberta, with an interest in communications and surveillance studies. He is currently studying the roles and responsibilities of internet intermediaries, including the responsibilities of internet service providers to facilitate surveillance, copyright enforcement, and cyber security.

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 53-62
Doi: 10.17645/mac.v3i2.297

Article

EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era

Nora Ni Loideain

Faculty of Law, University of Cambridge, Cambridge, CB3 9DZ, UK; E-Mail: nl301@cam.ac.uk

Submitted: 18 April 2015 | Accepted: 17 June 2015 | Published: 30 September 2015

Abstract

Legal frameworks exist within democracies to prevent the misuse and abuse of personal data that law enforcement authorities obtain from private communication service providers. The fundamental rights to respect for private life and the protection of personal data underpin this framework within the European Union. Accordingly, the protection of the principles and safeguards required by these rights is key to ensuring that the oversight of State surveillance powers is robust and transparent. Furthermore, without the robust scrutiny of independent judicial review, the principles and safeguards guaranteed by these rights may become more illusory than real. Following the Edward Snowden revelations, major concerns have been raised worldwide regarding the legality, necessity and proportionality standards governing these laws. In 2014, the highest court in the EU struck down the legal framework that imposed a mandatory duty on communication service providers to undertake the mass retention of metadata for secret intelligence and law enforcement authorities across the EU. This article considers the influence of the Snowden revelations on this landmark judgment. Subsequently, the analysis explores the significance of this ruling for the future reform of EU law governing metadata surveillance and its contribution to the worldwide debate on indiscriminate and covert monitoring in the post-Snowden era.

Keywords

Edward Snowden; EU law; human rights; judicial review; mass surveillance; metadata; personal data; privacy

Issue

This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction

Laws within democratic states prohibit public authorities from looking into the private lives of their citizens merely because they have the technological capacity to do so. The right to respect for private life and the protection of personal data underpin such national legal frameworks within the European Union (EU). Accordingly, the protection of this human right is key to ensuring that the oversight of State powers that permit the covert surveillance of communications for legitimate purposes (such as the prevention of terrorism and serious crime) is adequate and transparent. Moreover, without the robust scrutiny of independent judicial review, the principles and safeguards that ensure the effective application of this human right are at risk from becoming more illusory than real. Following the Edward Snowden revelations, major concerns were raised worldwide regarding the legality, necessity and proportionality standards governing State surveillance powers (Greenwald, 2014; Harding, 2014). Shortly thereafter in 2014, the highest court in the EU struck down the legal framework that imposed a mandatory duty on communication service providers to undertake the mass retention of their customers' metadata for up to two years in case this information may have assisted in the investigation, detection and prosecution of serious crime (Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger*). This article considers the influence of the Snowden revelations on this landmark judgment. The analysis begins by addressing the key factors that have contributed to the increasing importance of metadata for modern State surveillance. This examination then outlines the principles and safeguards guaranteed by the right to respect for private life under Article 8 of the international human rights instrument of the European Convention on Human Rights (ECHR) that apply to the covert surveillance of metadata by public authorities within the EU. The analysis thereafter discusses the origins, main provisions and controversy surrounding the legal framework that entrenched the mass and indiscriminate retention of metadata across the EU (section 2). Next, the article provides a brief overview of the Edward Snowden revelations with a focus on the covert mass metadata surveillance regime uncovered therein (section 3). The analysis subsequently turns to the main findings of the landmark judgment of the Court of Justice of the EU (CJEU/Luxembourg Court), the role of the Snowden revelations and the implications of this ruling for the EU legal order and data protection policy developments both within and beyond the EU (section 4). Lastly, the article concludes with a brief summary (section 5).

2. Metadata Surveillance

2.1. What Is Metadata Surveillance?

The term "metadata" relates to information generated or processed as a consequence of a communication's transmission. Much can be revealed from this data including: "latitude, longitude and altitude of the sender's or recipient's terminal, direction of travel…any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection" (Young, 2004). Metadata therefore concerns the *context* as opposed to the content of a communication and covers many types of information such as traffic data, location data, user data and the subscriber data of the device/service being used (e.g. cellular phone network or Internet service provider). As a result, metadata is a rich source of personal information as it reveals the "who" (parties involved), the "when", how long and how often, (time, duration and frequency), the "what" (type of communication, e.g. phone call, message, e-mail), the "how" (the communication device used, e.g. landline telephony, smartphone, tablet) and the "where" (location of devices used) involved in every communication we make. Moreover, the collection, aggregation and analysis of metadata can provide very detailed information regarding an individual's beliefs, preferences and behaviour.

In the 21st century, the depth and breath of information concerning an individual's private life that can now be revealed through the metadata surveillance of communications have advanced in tandem with dramatic technological developments.

Of particular note in this respect are two major changes regarding how society now communicates. First, there has been a distinct shift in the past century from the prevailing use of non-portable devices such as landline phones, faxes and personal computers to handheld smartphones and tablets. Secondly, major advancements in digitization and Internet access has led to the convergence of all of our communications (calls, e-mails, web searches, online shopping) to one device that is both mobile and Internet-enabled (Wicker, 2013). The constant trail of metadata left behind from the ceaseless use of these so-called "smart" communications devices facilitates the collection of unprecedented amounts of data and presents unique privacy challenges. As highlighted by the US Federal Trade Commission (FTC), "more than other types of technology, mobile devices are typically personal to an individual, almost always on, and with the user" (FTC, 2013).

Furthermore, given the increasingly ubiquitous use of mobile communication devices, these changes have made metadata surveillance just as valuable as (if not more than) the *content* of your communications for both law enforcement and commercial purposes. Consequently, the collection and processing of an individual's metadata can provide a level of monitoring of an individual's every communication and movement that was never attainable previously. For instance, Malte Spitz, a German Green Party representative, demonstrated the scope of this surveillance in a request to his mobile phone provider. Spitz sought a record of all the metadata collected and retained from the use of his mobile phone. Over the course of six months, this metadata tracked his geographical location and the use of his phone more than 35,000 times building a detailed narrative of his movements and his communications (Spitz, 2012). In other words, access to the content of our communications is no longer necessary to show what and whom we're interested in and what's important to us (Schneier, 2015).

2.2. Metadata Surveillance Threatens Privacy, Equality and Liberty

Unquestionably, the major technological developments outlined above have made the monitoring of metadata an essential and important tool for national security and law enforcement authorities around the world. The value of this surveillance was confirmed by General Michael Hayden, former director of the US National Security Agency (NSA) and the Central Intelligence Agency (CIA), who noted in a public debate concerning privacy and the NSA: "We kill people based on metadata" (Hayden, 2014).

However, indiscriminate mass metadata surveillance of entire populations by governments generates abundant amounts of personal data and consequently represents a substantial threat to the privacy, equality and liberty of individuals. This information can often be sensitive in nature and may identify many aspects of an individual's private life, including personal and professional relationships, racial or ethnic origin, political affiliations, religious beliefs, trade-union membership, financial status or medical history, to name just a few. The subsequent "aggregation" of this data into comprehensive online dossiers can reveal more to governments and private industry about an individual's identity and behaviour, than the individual may ever be aware of (Solove, 2008).

Accordingly, the creation, access and dissemination of such detailed digital profiles could result in insidious threats of computer-enhanced discrimination and manipulation that ought to raise considerable concern. The groups that face exclusion from access to opportunities (e.g. employment), goods or services based on data obtained from their Internet usage (particularly e-mail and web browsing) are less likely to be aware of their status as victims of categorical discrimination (Lessig, 1999). As a result, they will be even less likely to organize as an aggrieved group in order to challenge their exclusion from opportunities provided by the State or private sector (Gandy, 2003), thereby being prevented from asserting their constitutionally protected rights to privacy, equality and liberty.

2.3. Metadata Surveillance and the European Convention on Human Rights

Contracting States to the international human rights instrument of the European Convention on Human Rights (ECHR), who are also Member States of the EU, have argued in the past that the intrusion posed by metadata surveillance represents nothing more than a minimal interference with an individual's right to respect for private life (Ni Loideain, 2014a). However, since its leading judgment of *Malone* v. *United Kingdom* delivered in 1984, the European Court of Human Rights in Strasbourg (the international court established under the ECHR which reviews challenges to violations of the ECHR by Contracting States) has rejected this assertion.

Instead, the Strasbourg Court has consistently held that any processing (e.g. retention, access, analysis, storage, third-party dissemination) of metadata from an individual's communications (including telephony, e-mail, Internet usage) constitutes an interference with the right to respect for private life, as guaranteed under Article 8 of the ECHR. Moreover, the Strasbourg Court has subsequently upheld a number of challenges (*Valenzuela Contreras* v. *Spain* (1999); *Copland* v. *United Kingdom* (2007); *Liberty* v. *United Kingdom* (2009)) regarding the illegal use of these covert metadata surveillance powers by Contracting States. As will be examined below (see section 4.1), the highest court in the EU (CJEU/Luxembourg Court) would later close ranks with the approach of the Strasbourg Court in its landmark post-Snowden judgment of Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger*. The Luxembourg Court would do so by striking down an EU law that had raised human rights concerns within EU institutions and national courts across Europe since its inception.

2.4. Mass Metadata Surveillance and EU Law

Under the weight of considerable political pressure for increased counter-terrorism powers that followed the 9/11 attacks and the Madrid and London bombings in 2004 and 2005, the Data Retention Directive (2006/24/EC) was rapidly drafted, passed and entered into force by the EU legislature in 2006 (Murphy, 2012; Ni Loideain, 2011). The Directive provided that metadata derived from the communications of every natural person and legal entity within the EU must be retained and made available for the purpose of "the investigation, detection and prosecution of serious crime", as defined by each Member State in its national law. Specifically, this blanket measure imposed a mandatory duty on Member States to require private communication service providers to store and facilitate access to all of their customers' metadata to competent national authorities for up to two years. Under the 2006 EU Directive, this metadata concerned the devices used, the type of communication, the parties involved, their locations and the times and frequency of their communications. The broad scope of the Directive encompassed metadata from landline and mobile telephony, Internet access, Internet telephony and e-mail.

The EU legislature stated that the aim of the Data Retention Directive was to harmonize the varying domestic laws of EU countries concerning the retention of certain metadata by the private sector in order to ensure the availability of this information for the investigation, detection and prosecution of serious crime, as defined by each country under their national law. Nevertheless, many representatives of the EU Parliament, data protection authorities and NGOs across the EU consistently contested the compatibility of the Data Retention Directive with Article 8 of the ECHR and the EU Charter of Fundamental Rights. The EU Charter, effectively the EU's Bill of Rights, affirms the commitment of the EU to human rights and governs EU institutions and Member States when they are "implementing" EU law (EU Charter, Art.51(1)). Therefore, the scope of the EU Charter's application is much more narrow when compared to the US Bill of Rights as it does not impose a "federal standard" against which all national laws of the 28 Member States within the EU may be evaluated and set aside (Groussot & Pech, 2010).

The decision of the EU legislature to allow EU Member States to require the private sector to retain their customers' metadata for up to two years raised particularly major concerns. Previously, communication service providers would only keep this personal data for six months on average for billing purposes. There would have been some exceptions where information was held for longer if needed for the purpose of national security (Hawkes, 2006). Under the EU Data Retention Directive, however, storing this personal data for longer than six months was no longer the exception. Strikingly, no empirical evidence was put forward by any of the EU institutions to justify such a significant departure from the well-established principles of EU data protection law, particularly the tenet that personal data be retained for specific purposes within a scope that is necessary and proportionate. Even the Impact Assessment Report prepared by the European Commission, which served as the basis for proposing the Data Retention Directive, indicated that an upper maximum limit of only *one year* would be appropriate (European Commission, 2005). The Report warned that "a longer retention period would appear to be of little added value for law enforcement authorities while having important financial consequences for operators and [infringing] disproportionately on citizens' privacy".

Prior to its review by the CJEU in 2014, many of the highest national constitutional courts across the EU (Bulgaria, Cyprus, Czech Republic, Germany and Romania) had already upheld challenges striking down national provisions implementing the EU Data Retention Directive. The main grounds underpinning these judgments concerned the surveillance regimes' inadequate oversight and security standards and overall incompatibility with the legality, necessity and proportionality requirements mandated by the right to respect for private life, as guaranteed under Article 8 of the ECHR (Ni Loideain, 2014b).

3. The Snowden Revelations and Metadata Surveillance

Edward Snowden is a US citizen who now has temporary residence in Russia. He is a former computer analyst for the CIA and was subsequently employed as a defense consultant with *Booz Allen Hamilton*—a private management and technology consulting company contracted by the NSA. In June 2013 in Hong Kong, Snowden released thousands of US government records collected in his capacity at *Booz Allen Hamilton* revealing details of several programmes involving the mass surveillance of communications belonging to individuals both within and outside of the US to a select group of journalists in the UK and US news media, mainly *The Guardian* and *Washington Post* (Greenwald, 2014; Harding, 2014). Subsequently, news media outlets worldwide have also highlighted the questionable legality of US national security authorities sharing personal data obtained from these large-scale monitoring regimes with government authorities outside of the US (Article 29 Data Protection Working Party, 2014).

Among the many types of covert surveillance regimes that became public knowledge following the Snowden revelations, it came to light that one particular programme had been in operation for more than seven years. Similar to the EU Data Retention Directive, this monitoring involved the mass retention and access to metadata from the use of mobile phones for national security and law enforcement purposes. Following a court order issued under the Foreign Intelligence Surveillance Act 1978 (FISA), as amended, the Foreign Intelligence Surveillance Court required *Verizon* (one of the largest US communication service providers) to provide millions of phone records concerning its US customers on a daily basis to the NSA. This order included the telephony metadata of both US and non-US citizens as it applied to communications "(i) between the United States and abroad"; or (ii) wholly within the United States, including local telephone calls" (FISA Order, 2013). Although the duration of the FISA order was only for a three-month period, the same order had been the subject of renewal for seven years.

The revelations have prompted an ongoing global debate concerning the rapid pace of technological developments in the area of communications surveillance and the implications posed by this large-scale secret monitoring for individual's rights to privacy and the security of their personal data (Kuner et al., 2015). Furthermore, the revelations have also drawn attention to the significant role played by the private sector in the mass surveillance of communications for governments. Of notable controversy recently has been the question of whether governments should have a "back door" to the encrypted communications of the customers belonging to these private companies (Hayden, 2015). This issue has raised major concerns regarding the extent to which private actors should be co-opted into the blanket monitoring of individuals' communications for governments.

The subsequent complex debate on future law reform has resulted in a diverse range of responses from legal academics, the judiciary and the communication services industry in the EU and US. For example, in a report by the Review Group on Intelligence and Communications Technologies commissioned by US President Obama, the authors recommended that the bulk retention of metadata for State surveillance purposes should be the responsibility of communication service providers or other third-party private actors (The President's Review Group on Intelligence and Communications Technologies, 2013). In their view, storage by the government of bulk metadata creates potential risks to public trust, personal privacy, and civil liberty. However, the Grand Chamber of the highest court in the EU held the opposite in the landmark judgment of *Digital Rights Ireland and Seitlinger* shortly thereafter in April 2014. The CJEU struck down the 2006 EU Data Retention Directive for being in breach of the EU Charter of Fundamental Rights. As examined above (see section 2.4), this impugned EU law had imposed a mandatory obligation on all Member States of the EU several years earlier to require private communication service providers to retain the metadata of their customers for the investigation, detection and prosecution of serious crime for up to two years.

4. The Post-Snowden Era and the Landmark Judgment of the CJEU

4.1. Digital Rights Ireland and Seitlinger

The landmark judgment of *Digital Rights Ireland and Seitlinger* responded to requests from the High Court of Ireland and the *Verfassungsgerichthof* (Constitutional Court) of Austria that the CJEU examine the validity of the EU Data Retention Directive, particularly its compliance with the EU Charter of Fundamental Rights. Due to this metadata surveillance regime being an area of EU law, these courts were required to refer to the Luxembourg Court. EU law provides that national courts of EU Member States are unable to rule on the validity of EU legislation and therefore the constitutional courts of Ireland and Austria could not review the legality of the 2006 EU Directive (Case C-314/85 *Foto-Frost* v. *Hauptzollamt Lübeck-Ost* [1987] ECR 4199). Both proceedings arose from challenges to invalidate the national laws that implemented the EU Directive into Austrian and Irish law. Given the overlap of issues raised between the cases, the CJEU issued a joined response to both national courts. In a notable reflection of the reservations held by EU citizens towards this mass and indiscriminate retention of metadata, the reference to the CJEU from the *Verfassungsgerichthof* was the result of a constitutional challenge brought by more than 11,000 applicants (De Vries et al., 2011).

On 8 April 2014, the Luxembourg Court (sitting as a Grand Chamber of fifteen judges), seems to have acknowledged the human rights concerns raised by the national courts, data protection authorities and NGOs across Europe, by holding that the Data Retention Directive was invalid under EU law. The Court recognised the growing importance of metadata surveillance as “a valuable tool” for criminal investigations (para. 43 of the judgment). Nevertheless, the Court made clear that interfering “with the fundamental rights of practically the entire European population” for the legitimate objective of tackling serious crime does not justify surveillance regimes of the indiscriminate and unreasonable nature permitted under the Directive (para. 56). The Court criticized the starkly indiscriminate and therefore disproportionate scope of the Directive given that it applied to “all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime” (para. 56).

In particular, the Court took issue with the length of the retention period, that access by law enforcement authorities to data retained under the Directive did not depend on prior approval by a judge or another independent body and that the Directive did not explicitly require that Member States ensure that the private sector provide a high level of protection and security for the retained data (para. 66). The Court also highlighted that the Directive did not ensure the “irreversible destruction” of the data at the end of the retention period (para. 67). Additionally, in an uncharacteristic departure from its traditional minimalist approach, the Court addressed an issue that was not referred by either of the national constitutional courts. Specifically, the Court raised concerns regarding the location of the data retention under the fundamental right to protection of personal data guaranteed by Article 8 of the EU Charter. The Court held that the metadata retained under the Directive should have remained within the EU in order to fully ensure, as required under Article 8(3), the control “by an independent authority of compliance with the requirements of protection and security” (para. 68).

Based on all of the above grounds, the Court held that the “EU legislature had exceeded the limits imposed by compliance with the principle of proportionality” guaranteed under the fundamental rights to respect for private life and the protection of personal data under Articles 7, 8 and 52 of the EU Charter of Fundamental Rights (para. 69). By not limiting the temporal effect of its judgment, the Court declared the invalidity of the Directive to take effect *ab initio* (from the beginning), thereby erasing its entire existence from the EU legal order.

4.2. The Influence of the Snowden Revelations

Unquestionably, *Digital Rights Ireland and Seitlinger* is a landmark judgment likely to have reassured national courts of the EU’s commitment to fundamental rights. The judgment has also been lauded for confirming that high standards of privacy and data protection apply to the mass processing of personal data within the EU (Guild & Carrera, 2014; Lynskey, 2014). Despite the implications for other EU counter-terrorism policies, by invalidating the entire existence of the Data Retention Directive due to its incompatibility with the EU Charter, the Court “confirmed its commitment to an advanced system for the protection of human rights even in the context of national security” (Fabbrini, 2014). Furthermore, this is the first time that the highest Court in the EU has ever struck down an entire EU legal instrument due to its incompatibility with the EU Charter of Fundamental Rights.

Moreover, to the surprise of many, the Luxembourg Court in *Digital Rights Ireland and Seitlinger* also made a novel and major contribution to the EU legislative framework governing data protection, and for any future EU data retention measures. Notably, the Court appears to have effectively established that "data sovereignty' is a key element of the right to the protection of personal data guaranteed under Article 8 of the EU Charter of Fundamental Rights. Without this element, the Court stressed, the control by an independent supervisory authority of ensuring compliance with necessary data protection and data security requirements, required under Article 8 of the EU Charter, cannot be fully ensured. Strikingly, the Court did not limit the scope of this interpretation of Article 8(3) of the EU Charter to data retained under EU law for the purposes of tackling terrorism and serious crime, thereby making this requirement applicable to the retention of data pursuant to *any* EU legal measure. Accordingly, some commentators have gone as far as to note that the judgment could be interpreted as preventing the transfer of personal data to non-EU private and public bodies since access and use of this information would then be removed from the control of an independent supervisory authority, contrary to EU fundamental rights (Granger & Irion, 2014).

Consequently, the potential policy implications of the CJEU's interpretation of Article 8 of the EU Charter in *Digital Rights Ireland and Seitlinger* for the ongoing reform of EU data protection law are of considerable significance to public and private bodies both within the EU and beyond. By engaging so forcefully with an issue not referred by either of the national constitutional courts or decisive to the judgment, the Court's initiative in making this policy recommendation strongly suggests that the Snowden revelations played a role in the Court's assessment of the Data Retention Directive. While concerns relating to the need for data sovereignty between the EU and the US can be traced back to the 1970s, the emergence of the Snowden revelations has undoubtedly given impetus to a global debate on jurisdictional restrictions and the flow of personal data (Kuner, Cate, Millard, Svantesson, & Lynskey, 2015). To explicitly include a requirement of physical data retention within the EU under the EU Charter may result in major revisions to current provisions and exemptions under EU data protection law. In particular, such a requirement raises questions regarding the processing of data by the private sector and law enforcement authorities outside of the EU—a matter shortly to be before the Luxembourg Court in its review of the EU-US Safe Harbor Agreement.

4.3. Implications for the EU Legal Order and Beyond

A consensus among EU Internet regulation policymakers and scholars has emerged that the Snowden revelations have been influential in "emboldening" the approach of the highest court in the EU in its review of matters concerning privacy and data protection (Centre for European Legal Studies, 2015). Two landmark judgments delivered in the post-Snowden era by the CJEU support this contention.

First in April 2014 (as examined above), the CJEU struck down the entire legal existence of an EU law in *Digital Rights Ireland and Seitlinger* that entrenched a regime of mass metadata surveillance across the EU on the ground that it was incompatible with the EU Charter of Fundamental Rights. Furthermore, the highest court in the EU also surprised EU privacy scholars in its adjudication that data sovereignty forms part of the right to the protection of personal data guaranteed under Article 8 of the EU Charter of Fundamental Rights.

Secondly, shortly thereafter on 13 May 2014, the Grand Chamber of the Court delivered a second landmark privacy judgment where it established that EU citizens have a right to have links concerning them delisted from search engines that essentially encroach upon their private lives and the protection of their personal data (Case C-131/12 *Google Spain* v. *AEPD and Mario Costeja Gonzalez*). Specifically, the Court recognized a right under the 1995 EU Data Protection Directive (95/46/EC) for individuals to remove links generated by Internet search engines concerning searches for an individual's name which produce results that are "inadequate, irrelevant or no longer relevant, or excessive" (para. 92 of judgment). While the focus of *Google Spain* was not directly concerned with State surveillance, it nevertheless reaffirms the emboldened stance of the CJEU in matters affecting EU citizens' fundamental rights to respect for their private life and the protection of their personal data in the post-Snowden era.

Unlike the much-lauded *Digital Rights Ireland and Seitlinger*, however, it is important to note that *Google Spain* has divided academics, policymakers and the communication services industry worldwide. Some have gone so far as to describe the ruling as an infringement to the rights of access to information, freedom of expression and freedom of speech as it "opens the door to large scale private censorship in Europe" (CCIA, 2014). Others have argued that the practical impact of the so-called "right to be forgotten" (more accurately, the right to be delisted) will be comparatively limited in scope given the removal by search engines of links that involve millions of copyright violations on a monthly basis (Mayer-Schonberger, 2014). Notwithstanding the aforementioned concerns, it is important to highlight that *Google Spain* was an (albeit ill-conceived) attempt by the Court to address two important problems for the protection of privacy in the 21st century. First, "the Internet's ability to preserve indefinitely all its information about you, no matter how unfortunate or misleading" (Zittrain, 2014) and secondly, the enormous influence of search engines regarding your online (and inevitably offline) identity and reputation.

Unquestionably, however, both of these striking decisions delivered by the Luxembourg Court concerning the protection of the right to respect for private life and the protection of personal data since the Snowden revelations have strengthened the protection afforded by these human rights under EU law. The influence of the revelations for the protection of privacy through judicial review in Europe may extend further still in the future, given a pending application before the European Court of Human Rights in Strasbourg and in another related judgment pending before the CJEU in Luxembourg.

Both of these forthcoming human rights challenges concern the surveillance of personal data for national security and law enforcement purposes. The ongoing proceedings before the Strasbourg Court, *Big Brother Watch and Others* v. *United Kingdom* (App.58170/13), have been brought by three NGOs and Dr Constanze Kurz who allege that they may have been subject to surveillance by UK national security authorities in receipt of foreign intercepted material relating to their electronic communications. The applicants submit that this monitoring system (made possible by the PRISM, UPSTREAM and TEMPORA programmes revealed by Edward Snowden) violates their right to respect for private life, as guaranteed under Article 8 ECHR. In particular, the applicants assert that the requirements under the legality condition of Article 8 ECHR have not been satisfied by the UK legislature given that there is no statutory regime governing such surveillance and therefore there is an absence of adequate safeguards. Furthermore, the applicants contend that the "generic interception" of these external communications, merely on the basis that such communications have been transmitted by transatlantic fibre-optic cables, is an inherently disproportionate interference with the private lives of thousands, perhaps millions, of people.

The second set of proceedings pending before the CJEU in Luxembourg involves an Austria-based NGO (*Europe v Facebook*) which requested that the Data Protection Commissioner of Ireland issue proceedings against Apple and Facebook (both US companies have their European headquarters in Dublin) for violating EU data protection law by providing the personal data of EU citizens to the NSA. However, the then Commissioner, Mr Billy Hawkes, declined on the basis that both companies were parties to the Safe Harbor Agreement. This Agreement is a self-regulatory framework enforced by the US FTC and governs the exchange of personal data between the EU and US, thereby allowing US law enforcement authorities to access this information within the US. The Commissioner's decision was then challenged before the High Court of Ireland. Due to the implications of this judgment for the legal validity of the EU Data Protection legal framework, the national constitutional court referred the matter to the CJEU where oral hearings were held in March 2015. Specifically, the Irish High Court noted that the critical issue for the CJEU to determine concerns the interpretation of the 1995 EU Data Protection Directive and the decision by the European Commission in 2000 that under the Safe Harbor Agreement the US provides an adequate level of data protection. Both of these frameworks were drafted decades before social media became the increasingly ubiquitous form of communication that it is today, long before companies such as Facebook ever existed and before the EU Charter of Fundamental Rights became law in 2009. In light of the latter development, the Irish High Court seeks clarification from the CJEU regarding whether the 1995 EU Directive and the 2000 Commission's Safe Harbor Decision should be re-evaluated given the fundamental right of EU citizens to the protection of their personal data as guaranteed under Article 8 of the EU Charter (Case C-362/14 *Schrems* v. *Data Protection Commissioner*). It will be significant to see whether the Luxembourg Court will endorse the ongoing work of the EU legislature to reform and update the current Safe Harbor Agreement with the US Government (Kuner, 2015). Alternatively, the CJEU may adopt a more emboldened approach in assessing whether the role of the impugned Agreement within the EU Data Protection legal framework is compatible with the EU Charter of Fundamental Rights. Whatever the outcome, such major issues concerning the protection of EU citizens' rights to privacy and data protection would not be before the highest court in the EU if not for the Snowden Revelations which (as highlighted by the Irish High Court) formed the "backdrop" to this latest judicial review.

Finally, it is also important to note that the next test for the commitment of the EU legislature to EU fundamental rights compliance will be the future of the draft EU Directive on Passenger Name Records Directive (PNR Directive). This legislation seeks to harmonize the mass retention of personal data from travel information for law enforcement purposes across the EU. The proposed measure was revised to comply with the standards under Articles 7 and 8 of the EU Charter of Fundamental Rights, following the annulment of the Data Retention Directive by the CJEU in *Digital Rights Ireland and Seitlinger*. Although the European Parliament previously rejected the PNR Directive proposal in 2013, a revised draft of the PNR Directive is currently before the European Parliament (European Parliament, 2015). Although the scope of data retention under the draft Directive has been reduced, its proportionality remains highly suspect given the length of its retention periods—5 years for terrorism offences, 4 years for "serious transnational crime". It will be telling to see how much of a role the Charlie Hebdo attacks in Paris will play in how Parliament responds to the revised draft in this new political context. In other words, will the Parliament ensure that the revised PNR Directive meets the stringent human rights standards set out by the Luxembourg Court in *Digital Rights Ireland and Seitlinger*? Or, is it inevitable that this EU Directive will be subject to challenge for its lack of compliance with the EU Charter of Fundamental Rights before the CJEU in future?

5. Conclusion

In the landmark judgment of *Digital Rights Ireland and Seitlinger*, the highest court in the EU rightly erased from the EU legal order the imposition of a mass Internet metadata surveillance regime on Member States that had blatantly disrespected the privacy and data protection rights of more than 500 million EU citizens. This post-Snowden judgment marks the first time that the CJEU has ever struck down an entire EU legal instrument due to its incompatibility with the EU Charter of Fundamental Rights, thereby establishing greater certainty of an EU governed by a fundamental rights culture. Moreover, *Digital Rights Ireland and Seitlinger* established unequivocally that strict legality, necessity and proportionality standards must underpin the protection of privacy and data protection rights in all future EU legislation involving large-scale processing of personal data (including metadata).

Furthermore, the highest court in the EU also surprised EU privacy scholars in its adjudication that data sovereignty forms part of the right to the protection of personal data guaranteed under Article 8 of the EU Charter of Fundamental Rights. To explicitly include a requirement of physical data retention within the EU under the EU Charter may result in major revisions to current provisions and exemptions under EU data protection law. In particular, such a requirement raises questions regarding the processing of data by the private sector and law enforcement authorities outside of the EU—a matter shortly to be before the Luxembourg Court in its review of the EU-US Safe Harbor Agreement. The potential policy implications of the Court's interpretation of Article 8 of the EU Charter in *Digital Rights Ireland and Seitlinger* for the ongoing reform of EU data protection law are of considerable significance to EU and non-EU public and private bodies.

In addition to the striking down of the EU Data Retention Directive in 2014, the CJEU delivered a second landmark privacy judgment shortly thereafter. In *Google Spain*, the Luxembourg Court established that EU citizens have a right to have links concerning them delisted from search engines that essentially encroach upon their private lives and the protection of their personal data. Notwithstanding the understandable concerns raised by freedom of expression advocates prompted by the judgment, it is important to highlight that *Google Spain* was an (albeit ill-conceived) attempt by the Court to address two important problems for the protection of privacy in the 21st century. First, the indefinite and all-encompassing memory of the Internet regarding an individual's personal data and secondly, the enormous influence of search engines regarding an individual's online (and inevitably offline) identity and reputation.

Both of these judgments indicate that the Snowden revelations have been influential in emboldening the highest court in the EU in its review of matters concerning privacy and the processing of personal data by either public or private bodies. In particular, *Digital Rights Ireland and Seitlinger* has contributed to the enhanced protection of privacy and data protection in any future EU legislation involving mass metadata surveillance. Moreover, the influence of the revelations for the protection of information privacy through future judicial review proceedings in Europe may extend further still. Challenges to the compatibility of systems allowing for the covert access and monitoring of communications by US and EU national security and law enforcement authorities with Article 8 ECHR and Article 8 of the EU Charter of Fundamental Rights have been brought before the European Court of Human Rights in Strasbourg, and (again) before the CJEU. Hence, the Snowden revelations seem poised to embolden further jurisprudential developments and debate concerning the future of the legal standards and safeguards essential for the effective protection of privacy and personal data both within and beyond the EU.

Acknowledgments

I would like to express my thanks to all of my colleagues in the Faculty of Law at the University of Cambridge who shared their insights and observations on the above.

Conflict of Interests

The author declares no conflict of interests.

References

Article 29 Data Protection Working Party. (2014). *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*. Brussels: Secretariat of the European Commission.

Computer and Communications Industry Association (CCIA). (2014). CCIA's response to the European Court of Justice Online Privacy Ruling. Retrieved from https://www.ccianet.org/2014/05/ccias-response-to-european-court-of-justice-online-privacy-ruling

Centre for European Legal Studies (CELS). (2015). Podcast of Conference Proceedings "European Internet Regulation after Google Spain". University of Cambridge: UK. Retrieved from https://www.youtube.com/playlist?list=PLy4oXRK6xgzH6JjMA09uPmqOrahpPM9X https://itunes.apple.com/us/itunes-u/eu-internet-regulation-after/id986766672?mt=10 http://sms.cam.ac.uk/collection/1951973

De Vries, K., Bellanova R., De Hert, P., & Gutwirth, S. (2011). The German Constitutional Court judgment on data retention. In S. Gutwirth, Y. Poullet, P. de Hert, & R. Leenes (Eds.), *Computers, privacy and data protection* (pp. 3-23). Dordrecht: Springer.

European Commission. (2005). *Annex to the Extended Impact Assessment: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*. COM (2005) 438 final. Brussels: European Commission.

European Parliament. (2015, February 2), *Draft Parliament report on revised PNR directive proposal*. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE549.223+01+DOC+PDF+V0//EN&language=EN

Fabbrini, F. (2014). Human rights in the digital age. *Tilburg Law School Research Paper Series*, No.15/2014.

FISA Order. (2013). Verizon forced to hand over telephone data—Full court ruling. *The Guardian*. Retrieved from http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

U.S. Federal Trade Commission (FTC). (2013). *Mobile privacy disclosures: Building trust through transparency.* Washington, DC: FTC.

Gandy, O. H. (2003). Data mining and surveillance in the Post 9/11 Environment. In K. Ball & F. Webster (Eds.), *Intensification of surveillance* (pp. 26-41). London, UK: Pluto.

Granger, M., & Irion, K. (2014). The Court of Justice and the data retention directive in digital rights Ireland. *European Law Review*, *39*(6), 835-850.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the U.S. Surveillance State.* London, UK: Picador.

Groussot, X., & Pech, L. (2010). Fundamental Rights Protection in the EU post Lisbon Treaty. *Policy Papers of the Foundation Robert Schuman*, No.173/2010.

Guild, E., & Carrera, S. (2014). The political and judicial life of metadata: Digital rights Ireland and the trail of the data retention directive. *CEPS Paper in Liberty and Security in Europe*, No.65/2014.

Harding, L. (2014). *The Snowden files*. London, UK: Guardian.

Hawkes, B. (2006). The Data Retention Directive and data protection. *Privacy and Data Retention Directive Conference*, Irish Centre for European Law, Ireland. July 19, 2006.

Hayden, M. (2014). The price of privacy: Re-evaluating the NSA. *John Hopkins Foreign Affairs Symposium*. Retrieved from: https://www.youtube.com/watch?v=kV2HDM86XgI

Hayden, M. (2015). Getting past the zero-sum game online. *Washington Post*. Retrieved April 13, 2015 from: http://www.washingtonpost.com/opinions/dont-let-america-be-boxed-in-by-its-own-computers/2015/04/02/30742192-cc04-11e4-8a46-b1dc9be5a8ff_story.html

Kuner, C., Cate, F. H., Millard, C., Svantesson, D. B., & Lynskey, O. (2015). Internet Balkanization gathers pace: Is privacy the real driver? *International Data Privacy Law*, *5*(1), 1-2. doi:10.1093/idpl/ipu032

Kuner, C. (2015). Safe Harbor before the EU Court of Justice. *Cambridge Journal and Comparative Law Journal*. Retrieved from http://cjicl.org.uk/2015/04/13/safe-harbor-before-the-eu-court-of-justice

Lessig, L. (1999). *Code and other law of cyberspace*. New York, US: Basic Books.

Lynskey, O. (2014). The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety. *Common Market Law Review*, 51(6), 1789-1812.

Mayer-Schonberger, V. (2014). Omission of search results is not a “right to be forgotten” or the end of Google. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2014/may/13/omission-of-search-results-no-right-to-be-forgotten

Murphy, C. (2012). *EU counter terrorism law*. Oxford, UK: Hart.

Ni Loideain, N. (2011) Implications of the EC Data Retention Directive for data protection and privacy. In C. M. Akrivopoulou & A. Psygkas (Eds.), *Personal data privacy and protection in a surveillance era: Technologies and practices* (pp. 256-272). Pennsylvania: Information Science Reference.

Ni Loideain, N. (2014a). Surveillance of communications data and Article 8 of the European Convention on Human Rights. In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reloading data protection: Multidisciplinary insights and contemporary challenges* (pp.183-209). London, UK: Springer.

Ni Loideain, N. (2014b). Is the EU really about to outlaw mass metadata surveillance? *Wired.* Retrieved from http://www.wired.co.uk/news/archive/2014-04/28/mass-metadata-surveillance-eu

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York: W.W. Norton & Company.

Solove, D. J. (2008) *Understanding privacy*. London, UK: Harvard University Press.

Spitz, M. (2012). Your phone company is watching. *TEDGlobal Conference Presentation.* Retrieved from http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

The President’s Review Group on Intelligence and Communications Technologies. (2013). *The NSA report: Liberty and security in a changing world*. Princeton: Princeton University Press.

Wicker, S. B. (2013). *Cellular convergence and the death of privacy*. Oxford, UK: Oxford University Press.

Young, J. M. (2004). Surfing while Muslim: Privacy, freedom of expression and the unintended consequences of cybercrime legislation. *Yale Journal of Law and Technology*, *7*, 346-421.

Zittrain, J. (2014). Don’t force Google to forget. *New York Times*. Retrieved from http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0

About the Author

Nóra Ní Loideain
Nóra Ní Loideain B.A., LL.B., LL.M. (Public Law) is a PhD candidate in Law and CHESS Scholar at the University of Cambridge. Her doctoral thesis concerns the State surveillance of communications metadata in Europe. She is also a Research Associate for the Technology and Democracy Project in the Centre for Research in the Arts, Social Sciences and Humanities at the University of Cambridge. Previously, she was a Policy Officer in the Office of the Director of Public Prosecutions and Clerk for the Supreme Court of Ireland.

COGITATIO

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 63-76
Doi: 10.17645/mac.v3i2.279

Article

Subjunctive and Interpassive “Knowing” in the Surveillance Society

Sun-ha Hong

Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA 19103, USA;
E-Mail: shong@asc.upenn.edu

Submitted: 7 April 2015 | Accepted: 17 June 2015 | Published: 30 September 2015

Abstract
The Snowden affair marked not a switch from ignorance to informed enlightenment, but a problematisation of *knowing* as a condition. What does it mean to know of a surveillance apparatus that recedes from your sensory experience at every turn? How do we mobilise that knowledge for opinion and action when its benefits and harms are only articulable in terms of future-forwarded “as if”s? If the extent, legality and efficacy of surveillance is allegedly proven in secrecy, what kind of knowledge can we be said to “possess”? This essay characterises such knowing as “world-building”. We cobble together facts, claims, hypotheticals into a set of often speculative and deferred foundations for thought, opinion, feeling, action. Surveillance technology’s *recession* from everyday life accentuates this process. Based on close analysis of the public mediated discourse on the Snowden affair, I offer two common patterns of such world-building or knowing. They are (1) *subjunctivity*, the conceit of “I cannot know, but I must act as if it is true”; (2) *interpassivity*, which says “I don’t believe it/I am not affected, but someone else is (in my stead)”.

Keywords
belief; experience; imagination; interpassivity; media; mythology; ritual; surveillance; technology; uncertainty

Issue
This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. We Knew Already

At least, that was what some people said after Edward Snowden’s leaks on NSA surveillance. Did he tell us anything we didn’t know?, asked journalists (Milner, 2013). “They didn’t feel much like revelations”, said a director (Laskow, 2013). But what was meant by this curious phrase, *we knew already*? “Knew”—yes, some of the information really was public knowledge. But even the entirely new aspects of it were, apparently, not very surprising. After all, the discourse goes, we already “knew” of older NSA programs like Trailblazer and ECHELON—so we surely expected something like PRISM. But who is this “we”? The discourse designates a depersonalised hivemind: the knowledge of NSA surveillance was stored in our collective archive, though the proof is in nonhuman documents rather than what individuals can “remember”. Sometimes, the “we” instead designates the journalist, the director, the activist: the “we” in the know who pens these commentaries, the “we” that is less gullible than the average Joe, the “we” of the “we told you so”. And what about the “already”? Despite itself, the discourse is less about defining past concerns and more about characterising the present. It is a way to designate a historicity for the revelations—whether to dampen the outrage or stoke it. So: this *we* sure isn’t everyone, and sometimes excludes me at least; and the *knowing* it did certainly wasn’t a very comprehensive one. Satire, as it so often does, brings these ambiguities into the open: “We already knew the NSA spies on us. We already know everything. Everything is boring” (“We already knew,” 2015). What has knowing ever done for us, anyway?

These questions provoke and organise the present essay. I argue that what happened with Snowden was not a simple flip of the switch from collective ignorance to enlightenment. Rather, it is a question of what *knowing* involves. How do we develop belief about a surveillance system so vast it cannot be experienced by any single individual—and moreover, a surveillance system which consistently seeks to *recede* from lived experience? How is a "we"-that-knows interpellated, and how is this "knowledge" leveraged to authorise actions and opinions? It is often said that surveillance inherently violates our fundamental rights, and the public need only be informed in order to rise up against it. Others explain contemporary surveillance in terms of disempowerment, paranoia and anxiety (Andrejevic, 2013a; Bauman & Lyon, 2013; Browne, 2010). Yet for all the merits of such criticism, they sit uneasily with the fact that most people have learned to live *with* their awareness of Orwellian surveillance. Whether one seeks to defend state surveillance or denounce it, the basic operation that underlies both is a "world-building". The facts and arguments are cobbled together to present a new intuition, a new common sense, about how this enormous technological apparatus runs our world. Hence the question: how do we develop a sense of contemporary surveillance as a world "out there"?

In what follows, I first describe the *recession* of surveillance practices from the subject's lived experience. The gap created by this recession accentuates the role of speculation and belief. I then offer a conceptualisation of world-building vis-à-vis surveillance, drawing especially from phenomenology, affect theory and ritual theory. Finally, I discuss two common patterns in the Snowden affair discourse to indicate particular techniques of world-building. They are (1) subjunctivity, the conceit of *I cannot "know" but I must act "as if"*; (2) interpassivity, which says *I don't believe it/I am not affected, but someone else is (in my stead)*. These latter sections are based on ongoing research into the public discourse on the Snowden affair for a larger project. This essay draws on U.S. media coverage from June 6, 2013 (the date of the first leak) until March 14, 2014, focusing on prominent publications such as *The New York Times* and *The Washington Post*.[1] It also draws on high-profile public statements, such as Edward Snowden's public appearances and statements by President Obama or NSA personnel. The essay's arguments arise from identification of the recession of surveillance, and techniques for coping with that recession, in this body of discourse.

2. Recession

> People should be able to pick up the phone and call their family, should be able to send a text message to their loved ones, buy a book online, without worrying how this could look to a government possibly years in the future. (Edward Snowden in Rowan, 2014)

The irony is that many of us—including those outraged by NSA surveillance—*do* call our family, buy books online, and sleep very well at night. A few months after Snowden's appearance, a Pew survey (Rainie, Kiesler, Kang, & Madden, 2013) suggested that the majority of Americans believe their privacy is not well protected by current laws. Yet in most cases, their response amounted to deleting cookies. If the gesture was hopelessly inadequate, it at least had the virtue of being convenient. This apparent contradiction arises from the *recession* of surveillance. In contrast to the flood of media reports, actual surveillance technologies systematically withdraw from our lived experience and "personal" knowability. The mantra for this situation: "I know they might be watching, Edward Snowden told me so—but I don't 'experience' it."

We can first of all characterise this recession as technological. In a basic sense, all technology involves a withdrawal from sensory experience. Heidegger's hammer *externalises* human action and intention, and embeds it in a crafted object (Scarry, 1985). Computational technology often amplifies this recessive character. The smooth surface of the smartphone, even compared to the gears and chains on a bicycle, encourages us to *forget* the connections, dependencies and processes that maintain our environment—and should we remember, denies us easy access to that knowledge (Berry, 2011, Chapter 5). This is precisely the case with contemporary online surveillance. It is designed to operate behind the front-end user interface, sweeping up personal data out of human awareness. It interacts with the world—and us—in ways that our senses cannot access.[2] Even the physical databanks are literally isolated in a giant data centre in the Utah countryside. This is in distinct contrast to, say, American police surveillance. In that case, the post-1970's period has seen techniques like house raids, court summons, patrols, pat-downs and urine tests to impose state power viscerally upon the (especially poor black) population (Goffman, 2014). If in police raids or airport screenings (Adey, 2009; Parks, 2007; Schouten, 2014) surveillance intrudes rudely upon one's space, habit, affect and body programs like PRISM do the oppo-

[1] All relevant coverage from the following publications were examined: *New Yorker, The Atlantic, The Intercept, The New York Times, The Washington Post, Wired* (all online). *The Guardian* was also included as an especially relevant publication that was also read directly by many U.S. readers (which was not necessarily being true of *Der Spiegel*, another key player in the affair). Some snowballing was also conducted on the data for this essay.

[2] In Mark Hansen's (and through him, Whitehead's) vocabulary, recession is a question of phenomenological *access*. Surveillance is not only hidden in a traditional sense (classified, made a state secret); the technology itself is designed to operate at a sub-experiential level. See Hansen, 2015.

site. They evacuate every sign of their existence from lived experience. Consider the web beacon, commonly used in corporate/commercial surveillance. Also called tracking pixels, it is a tiny (1 × 1 single pixel), transparent object embedded into web pages to track user access. It is literally invisible to the naked eye, and the user may only discover it by bringing up the source code. Of course, even if I am informed of the existence of beacons and how they work, I quickly realise that it is impractical to comb through the source code of every page I visit. Momentarily armed with the power of knowledge, I surrender it again in favour of a deferred and simulated feeling-knowing: "I *would* be able to tell if a beacon is tracking me if I took the time to look."

The beacon illustrates the recession's epistemological properties. The subject is distanced from knowledge of surveillance at multiple levels. There is what we might call, in Rumsfeldian terms (Hannah, 2010), a "known unknown": I know *that* I will never know if an NSA agent has gone through *my* metadata. Then, there is the "unknown unknown": Snowden has revealed programs like PRISM and XKeyscore, but given the apparently enormous quantities of documents in Snowden's hands, and given that Snowden himself won't know everything, I now know *that* I am unlikely to ever know what I don't know about my vulnerability to surveillance. In Kafka's *The Trial,* what strikes Josef K. is not the fact that he is charged with serious crimes; it is that, despite every desperate attempt, the inscrutable bureaucracy yields no knowledge of what he is charged with and why. Certainly, Snowden's revelations have provided new information about state surveillance; "we" can say we "know" more than we had before. But we can see that this knowing can actually contribute to the recession of surveillance.

One ironic aspect of this recession is that most of us experience *discourse* about surveillance more than surveillance itself—a situation we also find with respect to globalisation (Cheah, 2008) and the nation-state (Anderson, 1991). Surveillance becomes available for talk and thought precisely *as* an estranged and phantasmal object. Through public, mediated discourse surrounding the Snowden affair, we make this surveillance into something knowable and sensible—even if the kinds of beliefs produced here are not strictly reducible to objective fact. This is what I mean by world-building activity. It is the interpellation of the surveillance society as a world "out there". Recession and world-building are intertwined. The former emphasises what we do not and cannot "know" for ourselves. The latter is how, despite this gap, we try to make some sense of the world we find ourselves in. Surveillance hides from us, but we cannot help but talk about it endlessly.

3. The "Out There"

Our ability to render surveillance society comprehensible is predicated not (only) on objective proof and available facts, but conventionalised ways for putting what we know together with what we don't know; ways for forming a coherent, though often inconsistent, picture. As noted above, many Americans—through media like Pew surveys—claim they are concerned about surveillance and often feel unsafe. At the same time, this same public has exhibited a clear willingness to live in and with this surveillance society, in many (not all) cases declining to take revolutionary or directly political action in response to the Snowden leaks. It is not sufficient to presume false consciousness, an illusory daze maintained by a clever concoction of ideology, misinformation and obfuscation. Studies into risk perception have shown that becoming better informed does not necessarily correlate to a stronger perception of dangers—or concrete actions taken to mitigate them (Douglas, 1992; Wildavsky & Dake, 1990, pp. 31-32). A similar sentiment is now being expressed by surveillance and privacy scholars. Subjects can know very well their rights are being violated and *live* with that violation (Andrejevic, 2013b; Mansell, 2012; Turow, 2013). The key is not to seek to unravel this "contradiction" into a consistent explanation, one which would supply us with a "worldview" with a singular internal logic. Subjects, Lauren Berlant tells us, are surprisingly good at managing their affective incoherence and disorganisation, and defending it in their own terms (Berlant & Edelman, 2014, p. 6; Berlant & Greenwald, 2012). When my firm belief in control over my life is challenged by news of state surveillance, or when my habituated attachment to new media bristles against my political views, I do not always respond with bold and sweeping changes to smooth out the differences. Rational consistency is often not our highest priority. Instead, what emerges is a set of platitudes, "common sense" wisdoms, habits, turns of phrase, speculative beliefs, recited facts, which support precisely the contradictions I have already come to embody. Now, this line of thought must be distinguished from older modernist denigrations of "primitive" beliefs. Those were presumed to be an amalgamation of non-scientific mistakes taken as eternal truths—thus explaining their resistance to rationalist "demystification". Here, it is a question of making knowledge of the world work *for* what subjects can't help but know, face, and deal with in their present lives. In short, to study world-building activity vis-à-vis surveillance is to understand how we *cope* (Berlant, 2011) with our own persistent living while under exposure to a relentless program of observation.

This isn't to say that nothing can knock us off from our serene perch. Crises happen—sometimes erupting in political and psychological drama, sometimes undoing social cohesion or individual well-being quietly in the backstage. Surveillance, too, can sometimes confront subjects violently and threateningly. The world-building perspective is to explain how things "work"—not perfectly, but sufficiently—in those times when crises *don't* happen, or when (possible) crises become dampened into compromises and apologies. The Snowden leaks certainly did challenge our previously built worlds. For some, it really was a crisis, driving them to explicit changes in behaviour. But many subjects also found ways to restore normalcy precisely by responding to new narratives and events, and rebuilding their positionality vis-à-vis the world out there. That is what we have always done, after all—even back when "we knew already". A great deal of knowledge about U.S. state surveillance had been available to the public before 2013. But this "we" had stumbled on ways to keep that knowledge sequestered in a dusty corner, a largely negligible and rather conspiratorial fact about "politics these days".

What these world-building responses suggest is that we have multiple ways of "knowing" and "believing". Indeed, those very terms do not do justice to that multiplicity. What does it mean to "know" when a teenager says "I know what I learned in school today", but can't articulate it to the expectant parent? What does it mean to "believe" in God but nevertheless demand scientific proof of his existence—or, inversely, accomplish my "belief" by submitting to Pascal's wager? As Žižek might quip, we know many "truths", but truths we are willing to die for, which we believe in absolutely in any circumstance, are all too rare. This is easier for us to grasp when we consider a nonmodern case. The Dorzé people in Ethiopia *believe* leopards are also Coptic Christian and observe fasting days prescribed by the religion…and on those fasting days, they will take care to protect their livestock from hungry leopards, as they've always done (Veyne, 1998, pp. xi-xii). They see nothing strange in this. Similar cases abound in anthropological writings. The Nuer believe twins *are* birds, which is distinct from saying birds are twins or that *this* twin is a bird (Douglas, 2001, p. 148). The key is to take on such contradictions not as mistakes or ignorance but as genuine world-building techniques. Or again: Merleau-Ponty (2012) argues that mythology or madness is not a case where our objective connectivity with the material world is underdeveloped or broken. Rather, a mythological explanation or a schizophrenic's hallucinations, *for those subjects,* involve a way of perceiving and understanding the world that is just as intuitive and genuine as our relationship to science, visual phenomena or speech. A schizophrenic woman believes two people with similar looking faces *must* know each other (Merleau-Ponty, 2012, pp. 298-299). This is an abnormal wiring of world-building capacity, but one which makes life possible and sensible for this woman in the same way something like physiognomy did normatively for 19th century urban dwellers (Pearl, 2010). The normal is full of arbitrary connections, too; one example is *confabulation,* or the pre-reflective and non-deliberate fabrication of personal memory that appears to occur in spontaneous ways to achieve self-understanding of what just happened (Orulv & Hyden, 2006).

In short, not only are our worldviews often complex and contradictory, we are also able to hold a plurality of relationships to the world out there through these flexible ways of knowing and believing. Why do we do this? Because contradiction and even incoherence can often be of great use in our ordinary living. Sometimes it's a matter of convenience, or of persuading others (and myself), of saving face. Sometimes we persist in some kind of belief because to jettison it would change our own image of ourselves unacceptably. The "effect" of a truth or belief is thus entangled with its "cause". To accuse such activity of inauthenticity is to miss the point. Such multiplicity is often critical to our ability to cope with our lived reality. It is what gives the subject the power to stay cohesive across the battery of situations and challenges it faces each day and hour—to maintain a feeling that despite everything, the world continues to make some minimal sense.

The next two sections will discuss concrete ways in which such world-building is taking place in the wake of the Snowden affair. They analyse how public debate is producing various narratives of the new surveillance world, and importantly, what specific ways of knowing and believing are involved in such production. The mass media plays what we might call a ritualistic role in this process. Media has been classified as ritualistic in the sense that media activity itself is often calendrical and collectively coordinated for effects of "liveness" and participation (Dayan & Katz, 1992). This effect is not reducible to the symbolic content of media coverage. Even if not everyone watches the same television program, even if interpretations of specific messages differ, even if some may not take media reports of the dangers of surveillance seriously, mass media have a *phatic* effect. The rhythmic pattern with which they take a place in our everyday life produces in itself a sense of connectivity to a wider world (Frosh, 2011). This phenomenological relationship enjoins the public not to swallow whatever they are told by the television anchor, but to continually adjust their position—sceptical, believing, critical, supportive—relative to media representations (Carey, 1975). It is on this basis that media performs itself as a "centre" of society, one which provides "*transcendent* patterns within which the details of social life make sense" (Couldry, 2003, p. 3). In other words, the media is less an indisputable source of factual statements about the world, than it is a repository of themes, topics and interests *against which* we form our beliefs about how the world works. One might decry surveillance coverage in the media as conspiratorial nonsense (of the Left, of the Right, of the American government, or the Russian one…) and disbelieve it; but that very move often entails *trusting* that coverage as some reflection of what “people out there” believe.

This leads back to the “we” of “we knew already”. Insofar as my sense of the surveillance world is framed in relation to what I believe is the *public* understanding and experience of surveillance, the public “out there” becomes an essential part of this mediated world-building. Indeed, the modern public, from its very inception in the age of the printing press, has always had a virtual and imagined quality. After all, what I can see and hear on my own is always only a small part of that human multitude, one which extends into the “out there” as an indefinite set of strangers (Eisenstein, 1980; Tarde, 1969; Warner, 2002). We learn to authorise ourselves to speak on the public’s behalf, or at least, *presume* what the public thinks and knows, in order to produce our own positions (Bourdieu, 1979; Hong, 2014). Media discourse, insofar as it is a ritualised promise of a “centre” of society, instructs its audience not only on what the public allegedly *is*, but how to relate to the public as an object of knowledge and belief (Fraser, 2006, pp. 155-156). Media discourse is thus the site where multiple ways of knowing and believing are expressed and legitimated, and it is on this basis that we are able to build a sense of surveillance as the world “out there”. We now move to two specific patterns: subjunctivity and interpassivity.

4. Subjunctivity

> Your rights matter because you never know when you’re going to need them. People should be able to pick up the phone and call their family, should be able to send a text message to their loved one, buy a book online, without worrying how this could look to a government possibly years in the future. (Snowden in Rowan, 2014)

> I buy fire insurance ever since I retired, the wife and I bought a house out here and we buy fire insurance every year. Never had a fire. But I am not gonna quit buying my fire insurance, same kind of thing. (James Clapper in Lake, 2014)

“You never know” is the ominous mantra that grounds both the claims of Edward Snowden, whistleblower, and of James Clapper, the U.S. Director of National Intelligence. “You never know” invokes a *looming*: a threat that is nothing *yet*, but is very much *real* in its existence as potential (Massumi, 2005, p. 35). The Orwellian future where you might be punished for your ordinary actions today; the apocalyptic scenario when terrorism happens to you and your family. That which by definition cannot ever be made certain is invoked as presumptively real in order to legitimise action—whether for or against state surveillance.

This is the *as-if*, the subjunctive. Grammatically, the subjunctive mood is the flotation of a non-true statement: “if I were…” This very construction produces an ambiguity, a split construction of “belief”. Such constructions *sustain* a state of affairs which is neither mere illusion nor fully believed to be true. In the Snowden discourse, we find the paradigmatic formulation of subjunctivity to be the *as if*: we must act, think, feel, believe, as if I am personally under watch, as if terrorism is about to happen *to me*, as if surveillance does help us prevent terrorism. In other words, the subjunctive involves a two-pronged handling of knowledge and belief, and this very ambiguity is what lets us *leverage* the unknown: “Yes, we don’t know if it’s true or not, but we have to pretend it is true”. It is telling that one of the few scholarly fields where subjunctivity is commonly discussed is in science fiction studies, centred on the work of Samuel R. Delany (1971). Although deployments of subjunctivity do not materially count as “events”, these characteristics mark them as highly ritualistic. Rituals have been called “time out of time” (Rappaport, 1999, pp. 216-222). They are moments when we collectively say, *wait*: let us step out of our rules and rhythms of life for a moment, so that they may be renewed and reaffirmed, or even, adjusted with localised change (such as the change in status of an individual member in a rite of passage). Similarly, the *as-if* is a way to step into a liminal (Turner, 1982) zone in one’s thinking and believing, but one which is then sutured back into one’s assessment of “reality”. It is a way for us to deal with our ignorance, our uncertainty, and other ways in which our present and ourselves in that present disappoint us. It is a way to *cope* with the imperfections and vulnerabilities of our exposure to power and danger.

This subjunctive turn in surveillance has been subject to much commentary. In risk literature, it is described in terms of “precautionary” or “catastrophic” risk—enormous uncertainties of climate change and terrorism which outstrip the industrial risks of factory disasters and chemical contaminations (Aradau & van Munster, 2007; Ewald, 1993). Surveillance studies frequently references Brian Massumi’s (2007) pre-emptive logic: a radicalisation of traditional causality and proof in a world of pure potentiality. My account does not necessarily supplant or contradict these theorisations. Rather, it emphasises the world-making aspects of subjunctive logic; a world-making which is capable of supporting both pro- and anti-surveillance attitudes.

The first type of *as-if* that permeates our present relationship to surveillance is the uncertainty about whether I am being watched at all. This effect is created by the juxtaposition of an apparently enormous and pervasive surveillance system, and, given its recession, the fact that the surveilled subject will rarely know if they have ever been “watched” by a human agent. Surveillance becomes a Deleuzian *virtual*. For Snowden and other opponents of NSA surveillance, it is critical to overcome this felt recession if the public is to “build” a world where surveillance is a keen danger. Ironically, this task is undertaken by combating another kind of as-if. Anti-NSA discourse consistently interpellate an imagined public, one which presumably thinks it is safe as long as it has not done anything "wrong". A *New York Times* op-doc, "Why Care About the N.S.A.?" opens thus:

> Narrator: I want to get your response to a few things people typically say who aren't concerned about recent surveillance revelations.
> David Sirota: Nobody is looking at my stuff anyway, so I don't care? My argument for that is if you don't speak up for everybody's rights, you better be ready for your own rights to be trampled when you least expect it. First and foremost, there are so many laws on the books, there are so many statutes out there, that you actually probably are doing something wrong….So when you start saying I'm not doing anything wrong…you better be really sure of that. (Knappenberger, 2013)

Sirota's warning is accompanied by a dizzying array of legalese in flight (Figure 1). By shifting the subject's gaze onto the bureaucratic and technological depths which almost entirely lie beyond everyday experience, the subject is divested of the ability to confirm or deny his/her own safety. This is distinct from the simple claim that we are not safe. It is (also) the claim that we do not have the ability or resources to *tell* in the first place. The projected "common sensical" subject is appealed to through an indeterminate "what if" situation, and *implicitly,* the argument is made that since the "what if" is particularly unsavoury, it should be considered as an "as if". Thus the reality of surveillance is impressed upon the subject not by recovering concrete surveillance practices from their recession, but actually by expanding their virtual dimension into an enormous, totalitarian as-if. Snowden and his sympathisers argue they are *informing* the public. True. But what they are also doing, above and beyond that, is to modulate an imagination which is necessarily in excess of the information strictly available.

This same technique is applied to the objective of surveillance itself: the threat of crime, and especially of terrorism. James Clapper quips that PRISM is no different from fire insurance. But insurance developed its appeal by quantifying fearful indeterminacy into percentages and premiums. The strategic use of disaster statistics and risk percentages could *claim* to provide a stable and objectively factual knowledge of danger and vulnerability. This is decidedly not the case with post-9/11 surveillance (Beck, 2009; Ewald, 1993). Terrorist attacks are sometimes analysed statistically, but their relative scarcity makes it difficult to draw convincing conclusions. The danger of being surveilled or falling victim to a terrorist attack is generally not parsed in terms of estimable "risks" (at least, not in public debate). As has been extensively analysed (and criticised), U.S. surveillance and anti-terror policy following September 11 has been predicated on the idea that even one attack is too much, and even one percentage a chance is too great (Aradau & van Munster, 2007; Cooper, 2006; Hannah, 2010). The proponents of state surveillance thus rely on the same "excessive" designation of the as-if. One key metaphor for NSA surveillance programs has been the *dragnet,* traditionally used to describe police activities like location-wide stop and frisks. The dragnet indiscriminately collects data on the innocent as well as the suspicious, highly relevant data as well as irrelevant ones—because the innocent can always turn out to be the criminal, and the most irrelevant piece of data may help triangulate his/her identity.

SUBCHAPTER III—INDIVIDUAL RIGHT OF ACTION IN CERTAIN REPRISAL CASES
SUBCHAPTER I—MERIT SYSTEMS PROTECTIO
(3)(A) The Board shall allow any agency which would be subject to a stay under this subsection
(B) Except as provided in subparagraph (C), a stay granted under
00:42
05:35
HD

Figure 1. "Why care about the NSA?"

Within this rationality, surveillance is not, strictly speaking, proven to be necessary by *past* terror attacks or *present* identification of concrete dangers. Proof is always deferred: we must act as if the efficacy of this program has been proven by a danger which, if we are right, we will prevent from ever actualising.

Subjunctivity is one name for how public figures *present* the world of surveillance. Importantly, this presentation is also a part of public subjects' wider, lived relationship to that complicated and distant world. And crucially, our relationship to the media *discourse* on surveillance itself becomes subjunctive as we try to navigate this tangle of complex and often contradictory claims. How can we produce a picture that makes sufficient sense to us, and how can we say to ourselves that we "know enough" to act, to not act, or at least to have an opinion about the whole affair? For instance, the subject's ability to assess the *legality* of surveillance becomes challenged by his/her experience of this discourse. Snowden's revelations were, at least, generally accepted in the media as solid, reliable information about the technical process of NSA surveillance. However, the precise legality of each given practice, and indeed, the question of *who* actually knows about and guarantees each practice, is explicitly designated as uncertain. As one headline put it: "You'll Never Know if the NSA Is Breaking the Law" (Bump, 2013). On one level, as David Sirota did above, it is suggested that there are so many different programs, legal decisions, secret courts and procedures involved, the public as a whole will "always" be left uncertain as to if the letter of the law is really being broken. On another level, we cannot presume that the reading public is a homogeneous mind with full access to every piece of information made available to them. The "we" of "we knew already" *does not exist* in such a form. Most subjects are likely to experience a partial picture, based on their limited reading and recall, of conflicting arguments and claims made in public. One may not keep up with every Snowden leak, tell apart XKeyscore from PRISM, or even understand exactly what counts as metadata and what doesn't. But it is more than possible to take away a general picture: the idea that the legality of surveillance is uncertain, and that any opinion or action we take will have to happen in abeyance of that knowledge.

What these situations suggest is that information often begets uncertainty, and in turn, provokes subjunctive responsivities. It is indisputable that Snowden's leaks have increased the total amount of knowledge we collectively hold about NSA surveillance. But the more Snowden reveals, the more cause we have for paranoia and uncertainty—an ironic reversal of Shannon's law of information. When we learn that the NSA monitors video game chatter for terrorist activity (Ball, 2013), it does not provide reassurance that we now know everything there is to know about that sordid affair. Rather, it gives us license to believe that if such a thing is true, *surely many more things might be as well.* Table 1 lists only the *major* additions to "our" knowledge of NSA surveillance between June 2013 and March 2014. It is quantitatively beyond what most subjects can afford to give full attention to. Indeed, the sheer number of documents Snowden has been said to possess—1.7 million by one count (Kelley, 2013)—makes the Snowden files themselves an inexhaustible and virtual repository of new revelations, just like the NSA's portfolio of surveillance technologies or the manifold dangers of the post-9/11 world. As with the question of legality, many subjects proceed with a general *awareness* that there is a plethora of leaks, without a firm grip on each leak or what they concretely add up to. Mary Douglas once asked: why do experts insist on educating the public about issues like climate change? Don't they realise that the more information becomes available, the more possible interpretations arise, and the more intractable a sensitive topic becomes? (2001, p. 146) To this, we might add: don't they know that information can feed speculation, rather than extinguish it? The Snowden leaks have provided additional ingredients for feeling uncertain and vulnerable. Whatever political position (including apathy and a "wait-and-see" prudence) one chooses, whatever imagination of surveillance one subscribes to, it must be predicated on an uncertain and receded reality that one chooses to overcome through the "as-if".

Finally, the subjunctive experience even extends to cases where subjects do try and take concrete steps to protect themselves from surveillance. While Edward Snowden espouses the benefits of programs like TOR, he admits:

> You will still be vulnerable to targeted surveillance. If there is a warrant against you if the NSA is after you they are still going to get you. But mass surveillance that is untargeted and collect-it-all approach you will be much safer [with these basic steps]. ("Edward Snowden SXSW," 2014)

Nearly every privacy solution recommended today comes with such caveats. As the concerned public flocked to existing privacy solutions, one VPN (Virtual Private Network) developer—a common alternative to TOR—commented:

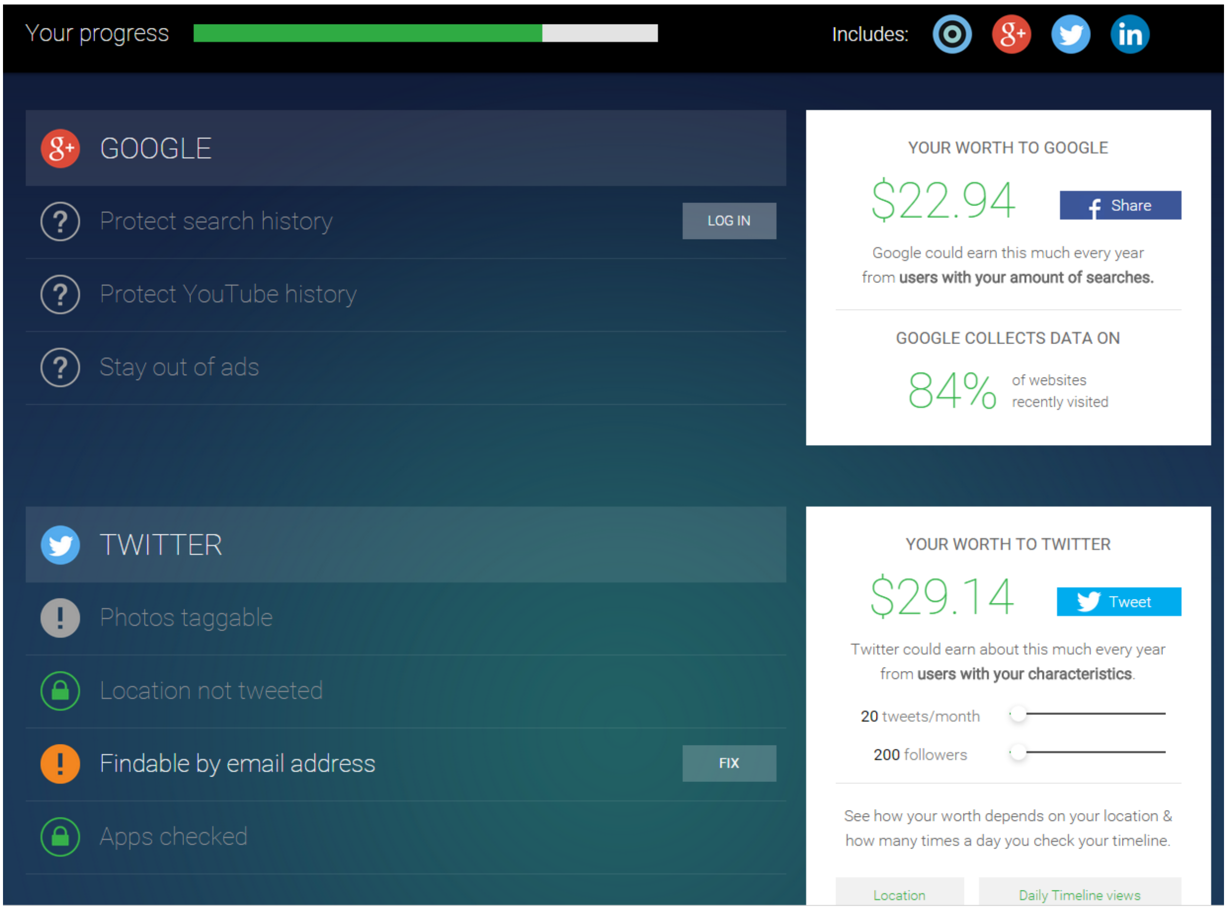
> If you're concerned about surveillance agencies such as the NSA, their capabilities are shrouded in secrecy and claiming to be able to protect you is offering you nothing but speculation. (Renkema, 2014)

Table 1. Major revelations on NSA surveillance, June 2013—March 2014.

14.3.12	Leak: NSA "Expert System" for malware implants allegedly planned
14.2.10	Leak: NSA metadata & geolocation helps drone attack
14.1.27	Leak: NSA uses "leaky" mobile apps
14.1.16	Leak: NSA collects millions of texts
13.12.13	Leak: NSA cracks cell phone encryption for A5/1 (2G standard)
13.12.10	Leak: NSA uses cookies to spy
13.12.9	Leak: NSA uses video games to spy
13.12.4	Leak: NSA collects 5 billion phone records per day
13.11.26	Leak: NSA spies on porn habits
13.11.23	Leak: NSA "Computer Network Exploitation" infects 50k networks
13.11.14	Leak: CIA collects bulk international money transfers
13.10.31	Leak: NSA hid spy equipment at embassies & consulates
13.10.30	Leak: NSA attacks Google & Yahoo data centres
13.10.24	Leak: NSA tapped 35 world leader calls
13.10.21	Leak: NSA spied on Mexico's Calderon, emails
13.10.14	Leak: NSA collects US address books, buddy lists
13.10.4	Leak: NSA can hack Tor
13.10.2	Leak: NSA stores cell phone locations up to 2 years
13.9.30	Leak: NSA stores metadata up to a year
13.9.28	Leak: NSA maps Americans" social contacts
13.9.16	Leak: NSA "Follow the Money" division tracks credit card transactions
13.9.7	Leak: NSA can tap into smartphone data
13.9.5	Leak: NSA attacks encryption standards and hacks
13.8.29	Leak: US intelligence "black budget"
13.8.23	Leak: NSA employees spy on ex-lovers
13.8.15	Leak: NSA internal audit shows thousands of violations
13.7.11	Leak: XKEYSCORE program.
13.7.10	Leak: NSA "Upstream" fibreoptic spying capacities
13.6.30	Additional PRISM leaks
13.6.19	Leak: NSA "Project Chess" for Skype
13.6.17	Apple, Microsoft, Facebook release details
13.6.16	Leak: NSA spied on Medvedev at G20, 2009
13.6.11	Leak: BOUNDLESS INFORMANT for surveillance records globally
13.6.10	Snowden named
13.6.9	Leak: NSA record/analysis tool
13.6.7	Leak: "Presidential Policy Directive 20" for cyberattacks to foreign targets
13.6.6	Leak: PRISM revealed

In other words, the subject's *feeling safe enough* is predicated on his/her ability to live on *as if* whatever tools chosen (including none) has provided sufficient protection against this unknown and silent risk. After all, one will never know if one's privacy *was* in fact compromised. The lived experience of interacting with privacy tools also contributes to this subjunctive situation. Consider AVG PrivacyFix (Figure 2), one of many simpler tools which promise to protect against (in this case, corporate) surveillance. It is all too easy: a few clicks, yellow and white symbols flashing into a reassuring green, and one is allegedly safer. Certainly, some of this software at least does provide some real mitigation against major surveillance techniques. But for any subject that is not particularly well informed or technologically savvy, the experience of using these programs is often a *simulation* of safety: a simulation against the inscrutable backdrop of a receded world. And so, even the subject who does "everything possible" to guard against surveillance must *subjunctively* reassure him/herself that "everything possible has probably been done".

The as-if is a technique for leveraging the receded, virtual enormity of "surveillance" to a produce a presumptive basis for knowing and believing. Such knowledge or belief is ambiguous and complex. One acknowledges the probabilistic or speculative nature of one's own belief, but simultaneously applies a practical—and sometimes even moral—injunction that hardens this belief and qualifies it for speech and action.



GOOGLE

Protect search history

Protect YouTube history

Stay out of ads

YOUR WORTH TO GOOGLE

$22.94

Google could earn this much every year from **users with your amount of searches.**

GOOGLE COLLECTS DATA ON

84% of websites recently visited

TWITTER

Photos taggable

Location not tweeted

Findable by email address

Apps checked

YOUR WORTH TO TWITTER

$29.14

Twitter could earn about this much every year from **users with your characteristics**.

20 tweets/month

200 followers

See how your worth depends on your location & how many times a day you check your timeline.

Figure 2. AVG PrivacyFix user interface.

5. Interpassivity

Interpassivity originally arose from art and media theory as a response to the dominion of "interactivity" (Pfaller, 2003; Scholzel, 2014; Van Oenen, 2002). It is now applicable as a more general conceit: "not me, but another *for* me". Someone else believes, so that even if I do not, it remains a kind of "truth" (Žižek, n.d.). I Xerox a book or VCR a television show, and become satisfied that I have *nearly* consumed it; in a way, the machine has "watched it for me" (Pfaller, 2003). This deferral, this "outsourcing" (Van Oenen, 2002), has numerous practical uses. Interpassivity allows us to maintain beliefs which may not be supported by our own behaviour, identity and environment. I don't believe Obama is Muslim, but there are people who do. I don't find this content morally offensive, but other people might. In such cases, the interpassive articulation *excuses* the subject from being bound to the belief in question, even as that belief is hypostatised into reality, thereby forming a reliable basis for opinions and actions. Indeed, in some cases, "delegating one's beliefs makes them stronger than before" (Pfaller, 2001, p. 37): my beliefs now appear as *objective* fact, something I cannot dismiss as mere flight of my fancy. We are familiar with this mechanism, of course, in the work of *rumour*. The conceit "I have heard it said elsewhere" holds the truthfulness of the rumour in constant suspense, adding to its resilience. I cannot vanquish a speaker who is there *in absentia.*

It is critical to understand what kind of "belief" is at stake in an interpassive movement. When I "act as if the Xerox machine were reading the text [for me]" (Pfaller, 2003), clearly, I do not "literally" believe that I have read the book. But I may well derive satisfaction from the act; a satisfaction that says "it is *almost* as if I have read the book, since I can now read it at any time I choose." When canned laughter laughs "for me" in a television sitcom, I do not look back and say "I now need not laugh." But, as Žižek (n.d.) points out, the experience can often leave me feeling "relieved" and rested afterwards. Such satisfaction is not necessarily reducible to false consciousness or pathological misrecognition. Interpassive techniques are ways for subjects to navigate a world which is so often alien to them, a world which they must nevertheless and constantly articulate as sensible and reliable. We employ interpassivity on a daily basis because it is a way to cobble together some understanding of politics, technology, public opinion, in the face of the harsh fact that so much of it exceeds our own experience and environment. The very ability to believe in surveillance as a part of our world is predicated on some noncongruence, some difference, between my "here" and the "out there".

Interpassivity was commonly leveraged in the

Snowden affair to mitigate precisely the recession of surveillance practices and knowledge from public debate. Indeed, certain "knowns" were quite explicitly evacuated out of the public domain and designated as "known elsewhere":

> Here's the rub: the instances where [NSA surveillance] has produced good—has disrupted plots, prevented terrorist attacks, is all classified, that's what's so hard about this. (Dianne Feinstein in Knowlton, 2013)

Feinstein and others insisted that the fruits of surveillance could not be proven publicly, lest that too endanger national security. Although one or two concrete cases have been mentioned (such as Najibullah Zazi's 2009 plot), the general trend was to claim that proof, too, was classified for the sake of security. Notably, these claims do not simply place the public in ignorance of "all the facts"; they demand that public deliberation take place *in full awareness of that ignorance*. It becomes impossible to simply say "the benefits of surveillance have not been proven", since proof has been publicly designated as existing elsewhere. Feinstein's apology asks the reading public to actively hold their judgment in abeyance, or to be precise, make their judgment by simulating what someone else knows in their stead. All this is compounded by admissions that even the special court tasked to know in our stead—a court that is itself secret—also judges in ignorance. Reggie Walton, the presiding judge of that very court at the time, explains:

> The FISC [Foreign Intelligence Surveillance Court] is forced to rely upon the accuracy of the information that is provided to the Court…the FISC does not have the capacity to investigate issues of noncompliance, and in that respect the FISC is in the same position as any other court when it comes to enforcing [government] compliance with its orders. (Leonnig, 2013)

The public is thus deprived of even the comforting thought that the law or the government "knows" in its stead. Rather, it is an indistinct other, dispersed and elusive, which promises to guarantee that surveillance indeed has been proven. This makes the interpassive movement fragile and speculative. When expert knowledge is stably instituted, the public can feel that it may reliably defer the work of knowing to those experts, and build a sensible world out of what the public itself does not know (Beck, 1992; Giddens, 1990). When expertise itself is threatened, as in climate change or the Snowden affair, the subject must make sense of what is happening in a more speculative and, indeed, subjunctive manner: "I don't know what the proof is, but if we presume for a minute that the proof is…" Even a cynical stance, which assumes that Feinstein and others are lying and there is no proof at all, requires some presumptive position to be taken against the knowledge that another has "for" me.

Certainly, the subject is not always forced to pretend to some knowledge of surveillance, interpassive or not. Nina Eliasoph's ethnography of Americans' everyday discussion of politics describes communities which consistently shy away from talking politics. When Eliasoph herself brought such topics up, it was seen as "an inert, distant, impersonal realm" too hard to get a handle on. It was a shame that political problems happened, and the "public" should do something about it—but that "public", the people who ostensibly knew enough to debate the problem, were not them (Eliasoph, 1998, pp. 131-135). Even the refusal to have an opinion was qualified by the interpellation of an other who participates in publics in my stead. The recourse to interpassivity is not reducible to voluntary "choice" by an autonomous agent. It is a responsivity demanded by a situation—a situation which comprises of the recession of surveillance, including the logic of secrecy and security folded into the debate.

Not only can the other know for me, but they can also *do* and *experience* for me. Since surveillance's pervasiveness far outstrips the highly infrequent occasions on which it intrudes tangibly into individual lives, interpassivity becomes a key technique by which a given political and affective orientation becomes fleshed out into our reality:

> My older, conservative neighbour quickly insisted that collecting this metadata thing she had heard about on Fox was necessary to protect her from all the terrorists out here in suburbia. She then vehemently disagreed that it was okay for President Obama to know whom she called and when, from where to where and for how long, or for him to know who those people called and when, and so forth. (Van Buren, 2013)

One might read this as typical liberal snarkiness about the cognitive dissonance of a stubborn conservative. But the general sentiment that there are people out there, "bad things" happening out there, that need to be watched and stopped is far from an abnormal one. Hence my own feeling of safety, my own ability to imagine a safer world, arises from a situation where someone else is surveilling someone else—myself, not being "that kind of person", one degree removed from the whole unpleasant affair. Indeed, interpassivity does not stop at projecting "probable factual events"; it also leverages downright fictional others. The non-news, fictional media thus participate in the ritualistic function:

> Great Britain's George Orwell warned us of the danger of this kind of information. The types of collection in the book—microphones and video cam-

> eras, TVs that watch us—are nothing compared to what we have available today. We have sensors in our pockets that track us everywhere we go. (Edward Snowden in "Whistleblower Edward Snowden gives,"2013)

Snowden's comparison might have been a little redundant. Sales of Orwell's *1984* had already rocketed by some 6,000% after his initial leaks in June (Hendrix, 2013). Of course, one cannot claim that the public flocked to Orwell, Dick and Huxley in order to take them literally as prophecy. But such fictional work clearly served as resources for making sense of the confused present and the uncertain future. Some of this imaginative media also intersected the contemporary surveillance debate with an older tradition of representing crime and police work. Jonathan Nolan's *Person of Interest* debuted in U.S. television in 2011, two years before the Snowden leaks. The series was nevertheless conceived through extensive consultation of U.S. state surveillance practices as was known and estimated at the time (Gan, 2013). The popular series presented the public with an NSA-style dragnet which "spies on you every hour of every day", which the protagonist would use each episode to track down individuals before they became perpetrators or victims of violent crime. On one hand, "The Machine", *Person of Interest*'s mass surveillance program, is clearly based on and evocative of U.S. state surveillance, providing the public with a simulation of hypotheticals. On the other hand, its show structure necessarily produces a world where urban crime of every kind proliferates and may strike *any* individual without notice. George Gerbner's famous cultivation theory suggested that media can have long-term, sedimented effects—that it can train people into presuming phenomena that lie beyond their own lives in order to, say, develop a heightened fear of criminal victimisation. This is not to say that *Person of Interest* is alarmist. The point is that insofar as terror and crime are not everyday realities for many (not all) of the population, we turn to fictional as well as strictly journalistic representations to develop an idea of what we can only assume is happening "out there". Nobody believes a television show is objectively true. But we often do leverage it for our world-building—just as we leverage the presumed opinions and actions of "others", and just as we leverage facts and statements we do not fully believe and cannot quite confirm.

6. Feeling-Knowing

Contemporary online surveillance is one which *recedes* in multiple ways from lived experience. This recession accentuates surveillance society's quality as a world *out there*: a vast, virtual entity which constantly eludes our knowing and living. Yet it is something which we invest a great deal of belief and passion into, cobbling what we know and suspect into a picture of a sensible, working world. The mediated public discourse on the Snowden affair exhibits two major techniques of such world-building. First, it leverages the virtuality and unknowability of surveillance *as if* it were in some way true and certain, producing hypothetical, provisionary bases for real, enduring actions and beliefs. Second, it encourages the notion that if *not me,* then another will know, experience, do in my stead. Even if the world of surveillance and terror is not real in my back yard, these interpellated others will make it real enough for me. The idea of the "public" or "society" provides a vast landscape of deferrals and potentials, a protective ambiguity for my political beliefs.

We began with a rhetorical question: "we knew already", didn't we? Well, what has knowing ever done for us, anyway? What matters at least as much as what we know or not, is what *kind* of knowing and believing has allowed us to engage that information. It is about what, affectively and epistemologically, it means to say 'I know'. Much has been made of the secrecy that surrounds state surveillance—the *arcana imperii*—and even corporate data-mining operations. The debate over Snowden as hero or traitor also revolves around this opposition of secrecy and transparency. Scholarly commentary often laments the ambiguous, uncertain and impoverished kinds of information the public is offered about surveillance. All of this is undoubtedly significant. But what this essay suggests is that we must also understand what techniques, what habits, of knowing and believing proliferate and become legitimated in this political environment. What wirings of narrative arcs, tropes, stereotypes, emotive associations, come into play in the discourse, images and practices of the surveillance society? It cannot simply be unrestrained paranoia or dangerousness. We use these symbolic ingredients not only to become afraid or suspicious, but also to cope with our subjection to surveillance, to make our daily routines and affects still make sense in this new world order. This line of questioning asks not what we know, but *how* we come to feel we know. And ultimately, it asks whether, given different circumstances, we could have a different relationship to knowing and believing surveillance.

Acknowledgements

The author would like to thank Carolyn Marvin, the anonymous reviewers, and the journal editors and staff at *Media and Communication.*

Conflict of Interest

This research received no specific grant from any funding agency. The author declares no conflict of interest owing to funding, employment or institutional membership.

References

Adey, P. (2009). Facing airport security: Affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space*, *27*(2), 274-295.

Anderson, B. R. (1991). *Imagined communities: Reflections on the origin and spread of nationalism* (Revised an.). London: Verso.

Andrejevic, M. (2013a). *InfoGlut: How too much information is changing the way we think and know*. New York: Routledge.

Andrejevic, M. (2013b). *What we talk about when we talk about privacy*. Paper presented at International Communication Association 2013, London, UK.

Aradau, C., & van Munster, R. (2007). Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations*, *13*(1), 89-115.

Ball, J. (2013, December 9). Xbox Live among game services targeted by US and UK spy agencies. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Cambridge: Polity.

Beck, U. (1992). *Risk society: Towards a new modernity*. London: SAGE.

Beck, U. (2009). *World at risk*. Malden: Polity Press.

Berlant, L. (2011). *Cruel optimism*. Durham: Duke University Press.

Berlant, L., & Greenwald, J. (2012). Affect in the end times: A conversation with Lauren Berlant. *Qui Parle: Critical Humanities and Social Sciences*, *20*(2), 71-89.

Berlant, L., & Edelman, L. (2014). *Sex, or the unbearable*. Durham: Duke University Press.

Berry, D. M. (2011). *The philosophy of software: Code and mediation in the digital age*. Basingstoke: Palgrave Macmillan.

Bourdieu, P. (1979). Public opinion does not exist. In A. Mattelart & S. Siegelaub (Eds.), *Communication and Class Struggle: I. Capitalism, Imperialism* (pp. 124-129). New York: International General.

Browne, S. (2010). Digital epidermalization: Race, identity and biometrics. *Critical Sociology*, *36*(1), 131-150.

Bump, P. (2013, June 28). You'll never know if the NSA is breaking the law — or keeping you safe. *The Atlantic*. Retrieved from http://www.thewire.com/politics/2013/06/nsa-surveillance-legal/66681/

Carey, J. (1975). A cultural approach to communication. *Culture and Communication*, *2*(1), 1-22.

Cheah, P. (2008). Cheah Pheng literature what is a world? On world as world-making activity. *Daedalus*, *137*(3), 26-38.

Cooper, M. (2006). Pre-empting Emergence: The Biological Turn in the War on Terror. *Theory, Culture & Society*, *23*(4), 113–135.

Couldry, N. (2003). *Media rituals: A critical approach*. Abingdon: Routledge.

Dayan, D., & Katz, E. (1992). *Media events: The live broadcasting of history*. Cambridge: Harvard University Press.

Delany, S. R. (1971). About five thousand one hundred and seventy five words. In T. D. Clareson (Ed.), *Sf: The Other Side of Realism* (pp. 130-146). Bowling Green: Bowling Green University Popular Press.

Douglas, M. (1992). *Risk and blame: Essays in cultural theory*. Abingdon: Routledge.

Douglas, M. (2001). Dealing with uncertainty. *Ethical Perspectives*, *8*(3), 145-155.

Edward Snowden SXSW: Full Transcript and Video. (2014, March 10). *Inside.com*. Retrieved from http://blog.inside.com/blog/2014/3/10/edward-snowden-sxsw-full-transcription-and-video

Eisenstein, E. L. (1980). *The printing press as an agent of change: Communication and cultural transformations in early-modern Europe, volumes I and II*. Cambridge: Cambridge University Press.

Eliasoph, N. (1998). *Avoiding politics: How Americans produce apathy in everyday*. Cambridge: Cambridge University Press.

Ewald, F. (1993). Two infinities of risk. In B. Massumi (Ed.), *The Politics of Everyday Fear* (pp. 221-228). Minneapolis: University of Minnesota Press.

Fraser, S. (2006). Poetic world-making: Queer as folk, counterpublic speech and the "reader." *Sexualities*, *9*(2), 152-170.

Frosh, P. (2011). Phatic morality: Television and proper distance. *International Journal of Cultural Studies*, *14*(4), 383-400.

Gan, V. (2013, October 24). How TV's "person of interest" helps us understand the surveillance society. *Smithsonian.com*. Retrieved from http://www.smithsonianmag.com/smithsonian-institution/how-tvs-person-of-interest-helps-us-understand-the-surveillance-society-5407171/?no-ist

Giddens, A. (1990). *The consequences of modernity*. Cambridge: Polity Press;

Goffman, A. (2014). *On the run: Fugitive life in an American city*. Chicago: University of Chicago Press.

Hannah, M. G. (2010). (Mis)adventures in Rumsfeld space. *GeoJournal*, *75*(4), 397-406.

Hansen, M. (2015). *Feed-forward: On the future of twenty-first century media.* Chicago: University of Chicago Press.

Hendrix, J. (2013, June 11). NSA surveillance puts George Orwell's "1984" on bestseller lists. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2013/jun/11/entertainment/la-et-jc-nsa-surveillance-puts-george-orwells-1984-on-bestseller-lists-20130611

Hong, S. (2014). The other-publics: Mediated othering and the public sphere in the Dreyfus Affair. *European Journal of Cultural Studies*, *17*(6), 665-681.

Kelley, M. B. (2013, December 13). NSA: Snowden stole 1.7 million classified documents and still has access to most of them. *Business Insider*. Retrieved from http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12

Knappenberger, B. (2013, November 26). Why care about the N.S.A.? *New York Times*. Retrieved from http://www.nytimes.com/video/opinion/100000002571435/why-care-about-the-nsa.html

Knowlton, B. (2013, June 9). Feinstein "open" to hearings on surveillance programs. *New York Times*. Retrieved from http://thecaucus.blogs.nytimes.com/2013/06/09/lawmaker-calls-for-renewed-debate-over-patriot-act/?_php=true&_type=blogs&_r=0

Lake, E. (2014, February 17). Spy chief: We should've told you we track your calls. *The Daily Beast*. Retrieved from http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html

Laskow, S. (2013, July 15). A new film shows how much we knew, pre-Snowden, about Internet surveillance. *Columbia Journalism Review*. Retrieved from http://www.cjr.org/cloud_control/a_new_film_shows_exactly_how_m.php

Leonnig, C. (2013, August 15). Court: Ability to police U.S. spying program limited. *The Washington Post*. Retrieved from http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html

Mansell, R. (2012). *Imagining the internet: Communication, innovation, and governance*. Oxford: Oxford University Press.

Massumi, B. (2005). Fear (the spectrum said). *Positions*, *13*(1), 31-48.

Massumi, B. (2007). Potential politics and the primacy of preemption. *Theory & Event*, *10*(2).

Merleau-Ponty, M. (2012). *Phenomenology of perception*. (D. A. Landes, Trans.). London: Routledge.

Milner, M. (2013, June 25). Did Edward Snowden tell us anything we didn't already know? *Chicago Reader*. Retrieved from http://www.chicagoreader.com/Bleader/archives/2013/06/25/did-edward-snowden-tell-us-anything-we-didnt-already-know

Orulv, L., & Hyden, L.-C. (2006). Confabulation: Sense-making, self- making and world-making in dementia. *Discourse Studies*, *8*(5), 647-673.

Parks, L. (2007). Points of departure: The culture of US airport screening. *Journal of Visual Culture*, *6*(2), 183-200.

Pearl, S. (2010). *About faces: Physiognomy in nineteenth-century Britain*. Cambridge: Harvard University Press.

Pfaller, R. (2001). Interpassivity and misdemeanors. The analysis of ideology and the Zizekian toolbox. *International Journal of Zizek Studies*, *1*(1), 33-50.

Pfaller, R. (2003). Little gestures of disappearance(1) interpassivity and the theory of ritual. *Journal of European Psychoanalysis*, *16*.

Pisters, P. (2013). Art as circuit breaker: Surveillance screens and powers of affect. In B. Pepenburg & M. Zarzycka (Eds.), *Carnal Aesthetics: Transgressive Imagery and Feminist Politics* (pp. 198-213). London: I.B. Tauris.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013, September 5). Anonymity, privacy, and security online. *Pew Research Internet Project*. Retrieved from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Rappaport, R. (1999). *Ritual and religion in the making of humanity*. Cambridge: Cambridge University Press.

Renkema, L. (2014, December 12). Which VPN services take your anonymity seriously? *Torrentfreak*. Retrieved from http://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/

Rowan, D. (2014, March 18). Snowden: Big revelations to come, reporting them is not a crime. *Wired*. Retrieved from http://www.wired.co.uk/news/archive/2014-03/18/snowden-ted

Scarry, E. (1985). *The body in pain: The making and unmaking of the world*. Oxford: Oxford University Press.

Scholzel, H. (2014). Beyond interactivity. The interpassive hypotheses on "good life" and communication. Paper presented at International Communication Association 2014, Seattle, USA.

Schouten, P. (2014). Security as controversy: Reassembling security at Amsterdam Airport. *Security Dialogue*, *45*(1), 23-42.

Tarde, G. (1969). *On communication and social influence: Selected papers*. (T. N. Clark, Ed.). Chicago: University of Chicago Press.

Turner, V. (1982). Liminal to liminoid. In V. Turner (Ed.), *Play, Flow, Ritual: An Essay in Comparative Symbology* (pp. 53-92). New York: Performing Arts Journal Publishing.

Turow, J. (2013). *Branded content, media firms, and data mining: An agenda for research*. Paper presented at International Communication Association 2013, London, UK.

Van Buren, P. (2013, January 13). 10 myths about NSA surveillance that need debunking. *MotherJones*. Retrieved from http://www.motherjones.com/politics/2014/01/10-myths-nsa-surveillance-debunk-edward-snowden-spying

Van Oenen, G. (2002). Interpassivity revisited: A critical and historical reappraisal of interpassive phenomena. *International Journal of Zizek Studies*, *2*(2).

Veyne, P. (1988). *Did the Greeks believe in their myths?*

An essay on the constitutive imagination. (P. Wissing, Trans.). Chicago: University of Chicago Press.

Warner, M. (2002). *Publics and counterpublics*. New York: Zone Books.

We already knew the NSA spies on us. We already know everything. Everything is boring. (2015, February 9). *Clickhole*. Retrieved from http://www.clickhole.com/article/we-already-knew-nsa-spies-us-we-already-know-every-1876

Whistleblower Edward Snowden gives 2013's alternative Christmas message. (2013, December 25). *Channel4.com*. Retrieved from http://www.channel4.com/programmes/alternative-christmas-message/on-demand/58816-001

Wildavsky, A., & Dake, K. (1990). Theories of risk perception: Who fears what and why? *Daedalus*, *119*(4), 41-60.

Žižek, S. (n.d.). The interpassive subject. Retrieved from http://www.egs.edu/faculty/slavoj-zizek/articles/the-interpassive-subject

About the Author

Sun-ha Hong

Sun-ha Hong is a PhD Candidate at the Annenberg School for Communication, University of Pennsylvania. His current research pursues uncertainty as a world-building resource in the new media society. Surveillance and data-mining's fixation with prediction and simulation show that such world-building involves a constant rearticulation of the unknown and the uncertain. For more, please see: http://sunhahong.org.

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 77-87
Doi: 10.17645/mac.v3i2.281

Article

The Role of Hackers in Countering Surveillance and Promoting Democracy

Sebastian Kubitschko

Centre for Media, Communication and Information Research, University of Bremen, 28359 Bremen, Germany;
E-Mail: sebastian.kubitschko@uni-bremen.de

Submitted: 1 April 2015 | In Revised Form: 25 June 2015 | Accepted: 23 July 2015 |
Published: 30 September 2015

Abstract

Practices related to media technologies and infrastructures (MTI) are an increasingly important part of democratic constellations in general and of surveillance tactics in particular. This article does not seek to discuss surveillance *per se*, but instead to open a new line of inquiry by presenting qualitative research on the Chaos Computer Club (CCC)—one of the world's largest and Europe's oldest hacker organizations. Despite the longstanding conception of hacking as infused with political significance, the scope and style of hackers' engagement with emerging issues related to surveillance remains poorly understood. The rationale of this paper is to examine the CCC as a civil society organization that counter-acts contemporary assemblages of surveillance in two ways: first, by de-constructing existing technology and by supporting, building, maintaining and using alternative media technologies and infrastructures that enable more secure and anonymous communication; and second, by articulating their expertise related to contemporary MTI to a wide range of audiences, publics and actors. Highlighting the significance of "privacy" for the health of democracy, I argue that the hacker organization is co-determining "interstitial spaces within information processing practices" (Cohen, 2012, p. 1931), and by doing so is acting on indispensable structural features of contemporary democratic constellations.

Keywords

big data; civil society organization; counter-power; democracy; hacker; locative media; media technologies and infrastructures; participatory media; privacy; surveillance

Issue

This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction: A Brief Outline of the Current Surveillance Scenario

Over the past decade, we have witnessed a drastic intensification of both the spread and use of media technologies and infrastructures (MTI). Education, work, politics, consumption, and socialization are but a few central spheres of life that are deeply infiltrated by digitization today. Practices related to or oriented towards MTI penetrate people's daily habits and routines to an unprecedented degree. This ongoing process has altered and, in many cases, multiplied people's ability to connect with each other, and has had a tremendous influence on the way people engage with the world at large (Couldry, 2012; Hepp, 2012). At the same time, networked technologies also enable a wide range of agencies and institutions to exercise control at a distance as well as to collect, sort, analyze and exploit the tremendous amounts of data that accumulate across mediated interactions. In many cases, this has resulted in a "collect everything" approach that is generally understood as surveillance; which, for now, is broadly defined as attention that is "purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence, or protection"(Murakami et al., 2006, p. 4). Surveillance, according to David Lyon, connotes any "collection or processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (2001, p. 2). One could look at the past decades and list both the beneficial and the problematic effects of technology. Yet, the story I want to tell in this article is somewhat more complicated and tries to avoid making overly sharp fractionations. Steering a middle ground in the current discussion on surveillance is by no means an easy task to perform as the debate is (over)loaded with accusations, idealizations, and a generous portion of ideology. This is particularly the case since Edward Snowden's revelations have expanded the notion of surveillance beyond a rather small expert discourse, and have instead catapulted the issue into the mainstream by increasing the level of media, public and political debate.

An accessible way to begin this analysis is to think about the spaces and places we experience surveillance first hand. Here, one might diagnose surveillance as a phenomenon that is most pressing in urban environments, as it is in the city and its surroundings where the highest number of surveillance forms and modes come together—video surveillance, license plate scanners, airports screenings, surveillance satellites and drones, as well as a number of other remote sensing and processing devices. Due to the invention and use of complex technical systems, it is no longer impossible to track and assess the simultaneous movements of tens of thousands of people through a major city. In fact, as scholars have argued convincingly, the ever-increasing surveillance in publicly accessible spaces, such as shopping malls, city streets and places for public transport, changes the ways in which power is exercised in urban space (Koskela, 2000). As a consequence, surveillance contributes to the production of the urban. The city is without a doubt a telling example that demonstrates that the intensification of digitalization often goes along with the amplification of surveillance (see Graham, 2004). Yet, as the above reference to contemporary MTI indicates, the "track record" of surveillance goes far beyond spatial and physical boundaries like urban environments. This, to acknowledge the history of the debate, is not necessarily a new observation as such. In his book on the impact of electronic data processing on personal privacy in the late 1960s, Jeremy Rosenberg stated that, "With the advance of technology, centralized data accumulation becomes easier, the reward for intrusion is increased, and control shifts to still fewer people" (Rosenberg, 1969, p. 1). Yet, times have changed drastically. In particular, the convergence and pervasiveness of MTI that have been developed and disseminated over the past two decades, enable surveillance attention to be continuous, widely distributed, and persistent. Considering today's vast (largely automated) computer power and the quasi-omnipresence of digital devices, the surveillance apparatuses that are currently in place, as well as those that are emerging and spreading, are historically distinctive.

In the following section, I will explicate what exactly makes our times distinctive by highlighting the delicate relationship between surveillance, privacy and the health of contemporary democratic constellations. I argue that hacker organizations like the Chaos Computer Club are one among a range of actors that counter-act contemporary assemblages of surveillance and by doing so act on indispensable structural features of democratic constellations. To develop this argument, the article is divided into three sections. In the first, I discuss three elements—popular online platforms, locative media and big data—that I consider determinative for contemporary surveillance contexts, and then analyze the increasingly symbiotic relationship between government agencies and corporations when it comes to surveillance tactics and practices. In the second section, I focus on the notion of privacy and why it matters for democracy at large. Finally, I use these concepts to examine a qualitative case study of the Chaos Computer Club.

2. Online Platforms, Locative Media and Big Data

Let me start by illuminating three elements that have intensified since the early 2000s and that have lastingly influenced both the way people experience surveillance as well as the way it is practiced. First, *popular online platforms*. The past years have seen an unprecedented triumphal march of a range of platforms that are often referred to as "social media" (see van Dijck, 2013). Considering the ambivalent evolution of the term—coming out of a business background—and the possible interpretation that all other media might be non- or even anti-social, I consider it more appropriate to use the term popular online platforms (see Gillespie, 2010) instead of social media. The main purpose of these platforms is to enable and simplify networking practices via mediated communication. To accomplish their goal, they heavily rely on personal data shared by the user. In accordance with this procedure scholars consider online "social networking" as a set of practices that are inherently based on self-surveillance (Fuchs et al., 2012). In addition, corporations make explicit use of online platforms to monitor and discuss strategies for responding to activists' initiatives (Uldam, 2014). In fact, popular online platforms have become part of people's daily routines to such an extent that they have become an imminent component of and an ideal environment for surveillance. This is not least the case because a small number of centralized communication platforms are much easier to browse, analyze and gain access to than decentralized infrastructures.

Second*, locative media*. With the transformation of mobile media from a communication tool into a multimodal device accompanied by global positioning systems enabling users to share information about one's whereabouts, locative media play a critical role in emerging modes of surveillance (Hjorth, 2013). Geotagging, location search and detection services amplified by portable and wearable devices like smartphones, tablet computers and smartwatches create new forms of co-presence that disrupt old binaries between online and offline (Schwartz & Halegoua, 2014). The potential to create new levels of surveillance is further enhanced by the fact that locative media intersect with online platforms in many ways because a growing number of services harvest their users' location information. Taking into account that it is exactly the way people use devices, platforms and services that create unprecedentedly large data bodies, scholars have argued that surveillance to a large extent has become participatory (Albrechtslund, 2008). One can sharpen this line of thought by pointing out that the rhetoric of the participatory turn actively exempts surveillance from legal and social control, resulting in a model of surveillance that is light, politically nimble, relatively impervious to regulatory constraint and even casts surveillance in an unambiguously progressive light (Cohen, 2015/forthcoming). Ironically, then, so-called participatory media are intimately connected with surveillance.

Third*, "big data"*. Big data—a notion that not only describes the sheer amount of data but also denotes automated, software-based data gathering, management and analytic capabilities—is best considered the missing piece to the puzzle called surveillance. After all, that is what surveillance is all about: solving a puzzle by bringing the fitting pieces consisting of data material together. Contemporary MTI allow for massive, latent data collection and sophisticated computational modeling (Tufekci, 2014). As Andrejevic and Gates write about the correlations of big data and surveillance: "Even if the underlying goal of capturing information for the pursuit of some form of advantage, leverage, or control remains constant, conventional understandings of the operation of surveillance and its social consequences are being reconfigured by the 'big data' paradigm" (Andrejevic & Gates, 2014, p. 185). Due to the need to interrogate vast quantities of data in very short times, surveillance tactics and strategies today necessarily rely on automated data collection, data analysis, and database management to correlate personal behavior, carve out relevant patterns and to extract metadata. Accordingly, big data is not only reliant on algorithms but also expands their regulatory power (see Beer, 2009; Bucher, 2012). While algorithms have been part of computing since the days of Turing, what we are currently witnessing is the marriage of (big) data and algorithms. One consequence of this convergence is the intrusion of algorithms in everyday life, which aim to analyze incredibly detailed physical, transactional, and behavioral data about people (Pasquale, 2015). Overall, big data play a critical role in turning many aspects of people's daily life into computerized data, thus enabling actors that have adequate resources to carry out surveillance on an unprecedented scale.

It is understood that all three elements—popular online platforms, locative media and big data—are far from disconnected from each other, but do inseparably interact with each other when it comes to surveillance. One can take popular online platforms as one example to explicate this entanglement. Given the enormous amount of interactions related to and oriented towards popular online platforms across the globe, these platforms are for the most part big data-driven media environments. At the same time, platforms today are increasingly accessed via location-based applications and devices. One can therefore conclude that surveillance as such is a big data endeavor (see Andrejevic & Gates, 2014; Tufekci, 2014). While the intimate relationship between technologies and surveillance goes at least back to evidence-producing tools like photography and telephone (Lauer, 2011), the pervasive embeddedness of media technologies and infrastructures in almost any spectrum of human life has introduced both a qualitative and quantitative difference. This observation echoes the principle that Shoshana Zuboff has convincingly outlined in her seminal writing on the *Age of the Smart Machine*: Everything that can be automated will be automated; everything that can be informated will be informated; every digital application that can be used for surveillance and control will be used for surveillance and control (Zuboff, 1988). To avoid misconceptions about this article's argument, it is important to stress that technology neither emerges out of nowhere nor does it exist in a vacuum (Garfinkel, 2001). More to the point, technology by itself does not practice surveillance; it is the actor—individual, collective, organizational, institutional—using particular technologies and the policies that set the legal frame that condition surveillance. Accordingly, it is important to note that technology also incorporates the potential for empowering citizens, making government transparent, and broadening information access (Howard, 2015). Then again, taking into consideration recent developments, this is not exactly the way things appear to evolve.

To start with, governmental surveillance and the objective to monitor citizens have a long history (Beniger, 1986). Not least since 9/11 and the declaration of the "war on terror", the desire of governmental agencies to monitor every possible communication channel has further intensified. Based on the argument that national security is at risk (Monahan, 2006), governments go as far as trying to make it legally binding for the tech-industry to install backdoors in their software and hardware. For the same apparent reason, some democratic governments even aim to explicitly counter anonymizing and cryptography services. In early 2015, Britain's Prime Minister David Cameron, for example, asked rhetorically: "[I]n our country, do we want to allow a means of communication between people…that we cannot read?". Most people in support of liberal democracy and who believe in the right of free expression would answer this question in the affirmative. Cameron in contrast stated: "My answer to that question is: No, we must not. The first duty of any government is to keep our country and our people safe" (see Temperton, 2015). Interestingly enough, in his crypto anarchist manifesto Tim May already indicates that "[t]he State will of course try to slow or halt the spread of this technology, citing national security concerns" (May, 1992). Here it is worth noting that "[c]ryptographic techniques have been providing secrecy of message content for thousands of years" (Chaum, 1981, p. 84). Governmental discourses, as David Barnard-Wills (2012) argues in his investigation of surveillance in the United Kingdom, tend to privilege surveillance as a response to social problems. Tellingly, "predictive policing", for example, is turning crime problems into a data problem. Most prominently three-letter agencies across the globe have been busy developing new methods and tactics to gain access to as much valuable information as possible. It is understood that in many cases these agencies collaborate across national boundaries. Interestingly, when it comes to surveillance, the often stark differences between democratic and authoritarian governments become more or less negligible (Gomez, 2004). Considering the concrete practices resulting out of such strategies it can be said that institutionalized politics makes use of surveillance amongst others to monitor, censor, classify, constraining free speech and even to put people in danger worldwide (Schneier, 2015). One might even go as far as to state that the government's control of informational infrastructures that make its territory and population legible has been a feature of the modern state since its birth (Beyer & McKelvey, 2015). All the same, the state is no longer the only or most powerful actor in the field of surveillance. During the 1970s and 1980s, the general assumption was that privacy problems stemmed from the centralized control of personal information held by governments in discrete data banks (Bennett, 2008). Over the past two decades, an increasing amount of personal information has moved into corporate hands (see Whitaker, 1999). More recently, corporations involved in the manufacturing and establishing of MTI have forcefully entered the field of surveillance as they have realized the monetary opportunities of data gathering, sorting, and processing. In fact, with the rise of the data-capture industry, surveillance is becoming more and more privatized and commercialized (see Ball & Snider, 2013). Cell phone providers track their customers' location and know whom you with. In-store and online buying behaviors are constantly documented, and expose if customers are sick, unemployed, or pregnant. E-mail communication and text messaging reveal sexual orientation as well as intimate and casual friendships. Based on estimated income level, interests, and purchase decisions, data broker corporations use surveillance for personalized advertisements, news articles, search results and persuasion (Couldry & Turow, 2014). Scholars refer to these conditions as "surveillance capitalism" (Zuboff, 2015) to underline the substantial scope of contemporary dynamics.

What is critical to note is that government agencies are important secondary beneficiaries of surveillance capitalism as they routinely access and exploit flows of data for their own purpose. In many cases governments directly offload the surveillance responsibility onto private-sector operators, as is the case in telephony and internet providers' legal obligation to store data for a minimum period of time. Overall, the borders between surveillance tactics that rely on government practices and those that rely on corporate activities become more and more obsolete, establishing a symbiotic public-private surveillance partnership. Not only are both camps drawing from the same interface and information, but their practices also augment each other. Again popular online platforms are one prominent example for this tendency as they reveal how individual, institutional, market-based, security and intelligence forms of surveillance co-exist with each other on the same site (Trottier, 2012). Surveillance is often illustrated as both a benefit for the development of Western capitalism and the modern nation-state (Murakami et al., 2006). As the Iranian-Canadian author and blogger Hossein Derakhshan stated after being released from a six years incarceration in Evin prison: "Being watched is something we all eventually have to get used to and live with and, sadly, it has nothing to do with the country of our residence. Ironically enough, states that cooperate with Facebook and Twitter know much more about their citizens than those, like Iran, where the state has a tight grip on the Internet but does not have legal access to social media companies" (Derakhshan, 2015). Corporate and governmental actors alike—each for their very own reasons—develop, maintain and exploit complex infrastructures for collecting, storing, evaluating and putting to use huge amounts of data to ultimately construct an absolute information awareness.

As the Snowden revelations have shown, surveillance often takes place without consent or agreement. At the same time, fitting the notion of participatory surveillance, scholars have stressed that much of surveillance is voluntary. To circumvent legal obstacles, like the Fourth Amendment in the United States and the European Union Data Protection Regulation, the data-capture industry relies on so-called voluntary disclosure of personal data; written into the terms and conditions that users constantly agree to without reading the incomprehensible, small-type, multiple page-long lists of rules. People actively participate in corporate surveillance because it promises convenience and rewards (Andrejevic, 2007). Millions of people wish to have their purchases tracked—and even complain when credit or supermarket affinity card transactions are missed—to accumulate frequent-flyer miles, loyalty discounts and other forms of “reward”. People to a large degree accept the routine collection of their data for the convenience of paying for a meal by credit card, or paying for a toll with an electronic tag mounted on their car (Garfinkel, 2001). As Simson Garfinkel puts is: “It’s a simple bargain, albeit a Faustian one” (2001, p. 5). Similarly, people willingly submit to government surveillance because it promises protection (Schneier, 2015). One informative case of continual voluntary self-surveillance is the quantified-self movement. While the earnest and geeky initiation of the “movement” by a group of technology evangelists was seeking better living through personalized control of data, commercial providers have increasingly entered the scene. The emphasis has therefore moved away from control over data towards the minutely quantified, intensively monitored, feedback-driven trajectories of self-improvement of health, diet, and fitness, as well as work habits, sex life, sleep patterns, and so on (Cohen, 2015/forthcoming). In 2014, Kolibree introduced a toothbrush that measures brushing patterns that transmit data to your smartphone to enable self-control as well as allow parents to monitor their children’s brushing. Also in 2014, for example, Generali—a German holding company consisting of about 20 insurance companies—introduced a new rate that allows customers to use an application to track their behavior, which transmits data to the insurance company. In return, customers who have a “healthier” lifestyle according to the company’s algorithmic evaluation receive special concessions.

Bringing the above-said together, it is reasonable to diagnose a strong tendency towards increased surveillance as well as the intersection of different forms and modes of surveillance. Surveillance—and its attendant apparatus, devices and systems—has become a central dispositif of our time (Bauman & Lyon, 2013; Gane et al., 2007). Today information flows and data monitoring on a mass scale produce a “surveillant assemblage” (Haggerty & Ericson, 2000, pp. 614-615) that predominately serves the interests of powerful entities, both private and public. Accordingly, contemporary tendencies complicate common conceptualizations of surveillance as discipline and control. Linking contemporary surveillance apparatuses with totalitarian political systems has become an oversimplified equation to make. “[T]he surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy” (Murakami et al., 2006, p. 1). Considering the way things have developed over the past decades, it is reasonable to assume that the coming years will see governments and corporations expanding their already effective assemblages of surveillance. Yet, as will be argued in the third section of this article, this does not exclude the fact that other actors like civil society organizations counter-act current tendencies. Before I will explicate this aspect, I will outline why all this actually matters when we think of the existing correlations between MTI and the health of democratic constellations.

3. Privacy and Why It Matters for Democracy at Large

The surveillance strategies and practices discussed previously put into question our deeply rooted sense of privacy. According to critical voices, privacy and datafication simply appear to be incompatible (Lane et al., 2014). Again, it is vital to stress that “privacy-invasive technology does not exist in a vacuum” (Garfinkel, 2001, p. 6). Taking into account the shifting field of actors involved in surveillance, Lane and her colleagues emphasize that data on human beings today are “less often held by organizations with traditional knowledge about how to protect privacy” (Lane et al., 2014, p. xi). The lack of privacy can become life threatening, for example in the case of journalists working in non- or pseudo-democratic countries. More generally, the lack of privacy puts into question the health of democracy *per se*. Aggressive and wide-ranging forms of surveillance preemptively decimate the possibility of a “right to be let alone”, as Gabriella Coleman (2014) has argued by referring back to Louis Warren and Samuel Brandeis’ (1890) classical conception. Warren and Brandeis, who were among the first to consider the basis of privacy law, defined protection of the private realm as the foundation of (individual) freedom. “Privacy” is by all means a deeply contested phenomenon, as the discourse and concerns about privacy have varied over time and definitions strongly depend on varying interests and agendas. All the same, researchers agree that current and emerging technological developments in data processing pose serious challenges to societies as they destabilize the delicate balance between privacy, security, autonomy and democratic rights.

In this context, a helpful conception of privacy is the approach that privacy is the “claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (Westin, 1967, p. 7). Privacy, in other words, is something that every human being is in need of to some degree. To avoid misconception, it is important to note that privacy here is not understood as a reinforcement of liberal individualism, but as a phenomenon critical for societal arrangements as a whole. In other words, the question for the relevance of privacy is framed in social terms and conceptualized as an explicitly political issue. In this context, Julie Cohen’s (2012) article on what privacy is for contributes a rich set of arguments to the discussion. As she puts it: “Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops”

(Cohen, 2012, p. 1905). Accordingly, for Cohen, "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is an indispensable structural feature of liberal democratic political systems" (Cohen, 2012, p. 1905). Conditions of diminished privacy seriously weaken practices of citizenship as "[p]rivacy isn't just about hiding things. It's about self-possession, autonomy, and integrity" (Garfinkel, 2001, p. 4). Seen from this perspective, privacy incursions not only harm individuals' capacity for democratic self-government, but also jeopardize the continuing vitality of political and intellectual culture at large (Cohen, 2012, p. 1906). Tim Berners-Lee, the inventor of the World Wide Web, recently stated that the extension of surveillance powers translate into a "destruction of human rights" (Katz, 2012). Ultimately, as Cohen remarks, "A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy" (Cohen, 2012, p. 1912). In more practical terms, privacy plays important functions within democratic constellations by promoting, amongst other things, the freedom of association, shielding scholarship and science from unnecessary interference by government, permitting and protecting secret ballots, and by serving as a shield for those actors that operate to keep government accountable (Westin, 1967). All in all, the politics around privacy are critical for the constitution of democracy.

Let me now bring this conception of privacy into dialogue with the earlier-discussed elements concerning the pervasiveness of contemporary MTI that co-determines both people's practice of and the capacity for citizenship. A large portion of participatory MTI today aim to turn people into predictable citizen-consumers whose preferred modes of self determination play out along revenue-generating trajectories (Dean, 2009). Along with the spread of MTI, public and private regimes of surveillance have become an ordinary and mundane process that in many cases narrows critical citizenship and opportunity for it to flourish. "Imbuing our networked information technologies with a different politics will require both the vision to appreciate privacy's dynamism and the will to think creatively about preserving it" (Cohen, 2012, p. 1933). By implication, the widespread—if not even omnipresent—construction of systematic surveillance apparatuses fundamentally changes conceptions of what it means to be "visible" or "in public" (Haggerty & Ericson, 2006). This is particularly highlighted by scholars that explore the ways that exposure within surveillance assemblages affects both identity and resistance (Ball, 2009). Privacy prevents the absolute politicizing of life and protects the ability of actors to develop their identity as well as to voice their concerns freely across media environments.

In summary, the literature on surveillance leaves us with the convincing argument that the quantity and quality of monitoring have changed drastically over the past decades. One not only witnesses increasing surveillance and decreasing privacy, but also that current and emerging surveillance assemblages have fundamentally altered people's experience of and interactions with MTI. It is further reasonable to assume that the lack of privacy is harmful materially, psychologically, socially, and politically. After taking into account the arguments of the above-mentioned scholars, it becomes clear that discussing surveillance is also an examination about the health of democratic constellations. On a more theoretical level, one can distill that as surveillance merges into a corporate/government joint venture and shifts towards a participatory phenomenon, established conceptualizations of surveillance as discipline and control appear obsolete. So far, the array of actors that researchers and journalists alike have focused on are the state and the corporate sector as well as their consolidation (Ball & Snider, 2013; Beniger, 1986). Similarly, the worrying correlations between participatory media and surveillance have also gained considerable scholarly interest (Albrechtslund, 2008; Fuchs et al., 2012). Likewise, writings discussing the societal relevance of whistleblowing and activists' data leaks—both aspects that are connected to privacy—have emerged recently (Brevini et al., 2013). What has been much less noticed and investigated, however, is the role played by actors who counter surveillance.

This is all the more astonishing, considering the fact that due to all-encompassing surveillance, the question asking who is acting "against" surveillance is ever more pressing. In his seminal warning about the steady slide toward the surveillance society, Lyon (2001, pp. 131-135) has argued that sustaining privacy depends less on mechanisms devised and implemented by elites, and more on the extent to which resistance to surveillance practices are enacted through movements and organizations in civil society (see Bennett, 2008). To discuss exactly this issue is the aim of the following section. Throughout the third part of this article, I will therefore present findings from qualitative research that has been conducted on the Chaos Computer Club (CCC)—Europe's largest and one of the world's oldest hacker organizations—from 2011–2014. The data presented in this article is based on 40 face-to-face interviews, numerous participant observations at public gatherings, hackerspaces, hacker conventions and private get-togethers as well as on a media analysis that took into account self-mediation, practices, media coverage and different forms and styles of media access. I aim to make a convincing argument that the CCC counter-acts contemporary surveillance assemblages in two ways: first, by de-constructing existing technology and by supporting, building, maintaining and using alternative media technologies and infrastructures that enable more secure and anonymous communication; and second, by articulating their expertise related to contemporary MTI to a wide range of audiences, publics and actors. The hacker organization here stands representatively for a growing network of activists that feel ambivalent and uncomfortable towards the affordances of MTI to be used as a surveillance apparatus.

4. Counter-Acting Surveillance Assemblages

Since the year of its foundation in 1981, the CCC considers itself a non-governmental, non-partisan, and voluntary based organization that is involved in framing media technologies and infrastructures as political phenomena relevant to society at large. The hacker organization explicitly conceptualizes MTI as being embedded in complex power dynamics and act accordingly (Kubitschko, 2015a). After a brief identification stage, the collective registered as a nonprofit organization in 1984 and started to promote their political endeavor of advancing more secure communication and information infrastructures more explicitly. In addition, as a registered lobby group, the Club advocates for more transparency in government, communication as a human right, and free access to communication and information infrastructures for everyone. Colin Bennett (2008) has referred to these kinds of actors as privacy advocates that resist the spread of surveillance and in fact explicitly lists the Chaos Computer Club as a privacy advocacy organization. Ever since the late 1990s, the Club has seen an exponential rise of membership that today figures around 5500 members. To explicate the argument that the hacker organization is acting on indispensable structural features of contemporary democratic constellations, this article will focus on the Club's engagement since the early 2000s. Focusing on a specific time frame also allows us to concentrate on an episode when the three above-mentioned elements—popular online platforms, locative media and big data—were coming to life ever more prominently.

To start with, the CCC, of course, does what one might primarily expect from a hacker organization: hacking. Yet, it is worth emphasizing that hacking can take many different forms. In the context of the research presented here, hacking is understood as critical, creative, reflective and subversive use of technology that allows creating new meanings. This kind of engagement goes back to the early days of the CCC and has intensified over the past decade. One of the recent example is the CCC's so-called Federal Trojan hack in 2011. By disclosing governmental surveillance software that was used (unconstitutionally) by German police forces, the Club initiated a heated political debate about the entanglements of technological developments and state surveillance in Germany. This was two years before the issue of surveillance gained global currency owing to Snowden's revelations about the US National Security Agency (see Möller & Mollen, 2014). Here it is helpful to note that the notion of "data protection", which is derived from the German Datenschutz, entered the vocabulary of European experts in the 1960s and 1970s at about the same time as the notion of informational or data privacy arose. Germany, in other words, can generally be considered a surveillance aware nation. The notion of Informationsselbstbestimmung (informational self-determination), for example, has constitutional status in Germany. This example shows that hacktivism, as hackers' political engagement is generally entitled (see Jordan & Taylor, 2004), does indeed include digital direct action (Coleman, 2014). Hacking in the case of the Federal Trojan means acting as a watchdog of governmental agencies by uncovering surveillance tactics and practices. By deconstructing the abstractness of a given technology—surveillance software in this case—the CCC materializes its formerly unrecognized political quality.

Another principal set of hacker practices to counter-act surveillance assemblages is the CCC's financial, social and technical support of infrastructural projects that establish alternative information and communication environments. That is to say, the CCC aims to contribute to create (more or less) uncontrolled spaces where the regulation of the state and the interests of corporations cannot intrude. Developing anonymous communication spaces for citizens has been a project deeply embedded in hacker cultures for some time. The reasons and ideologies of so-called cryptowarriors, for example, differ, but they align in the desire and development of tools that might ensure to enhance privacy (see Greenberg, 2012). In practice, this means that besides critically engaging with technological artifacts the CCC puts a lot of effort into building, supporting and maintaining alternative infrastructures that enable more secure and anonymous ways of communicating outside the realm of data-hungry, profit-oriented assemblages. During the 2008 Beijing Olympics, for example, the Club provided a manual and matching tools enabling journalists and other interested users to circumvent online censorship and surveillance by allowing people free access to information and communication. At the time of research, the hacker organization was operating five Tor servers and was running one of the most used XMPP servers in the world. The Onion Router (Tor) is an overlay network that has its roots David Chaum's (1981) notion of mix networks and is best considered a privacy enhancing technology. More concretely, it is a client software that enhances online anonymity by directing internet traffic through a volunteer network of special-purpose servers scattered around the globe. The Extensible Messaging and Presence Protocol (XMPP), formerly known as Jabber, is an open technology that includes applications like instant messaging, multi-party chat, voice and video calls. "The right to privacy includes the right to anonymity. The only way to protect this right is to exercise it" (Garfinkel, 2001, p. 172). The two systems are designed to protect people's anonymity while browsing the internet and to conceal information from unwanted listeners. The design of Tor and XMPP makes it difficult—and potentially even impossible—for governments to seize the content or to eavesdrop on the interactions. It is important to mention that Tor and XMPP might be considered alternative MTIs, but this does not necessarily imply that they are autonomous in an absolute sense, as they still depend on the commercial internet backbone like cables and internet exchange points. At the same time, these are initiatives that constitute serious alternatives to existing profit-driven online services highlighting that cryptography can be a powerful tool for controlling the unwanted spread of personalized information. The Club's aim is to set limits on surveillance assemblages by making anonymous access as the standard mode of operation across the network's architecture.

Tor is amongst others widely used by journalists and human rights activists who feel the need to conceal their identity due to the drastic penalties that their publications might imply in their home country. Similarly, most aspects of whistleblowing today would be unimaginable without anonymizing services. Encryption is an effective way of avoiding feeding surveillance assemblages with data. Some cryptography enthusiasts go as far as arguing that the technology is a silver bullet for achieving universal privacy, solving virtually all of the problems posed by contemporary surveillance assemblages. Tim May explains in his manifesto, which he read at the first cypherpunk founding meeting in 1992 in Silicon Valley, and later posted to the group's electronic mailing list: "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner" (May, 1992). According to May, "crypto anarchy" would, among other things, "alter completely the nature of government regulation,…the ability to keep information secret, and will even alter the nature of trust and reputation" (May, 1992). Yet, it is important to note that cryptography does not necessarily protect privacy, but also protects information (Garfinkel, 2001). What cryptography does in the first place is to guarantee the confidentiality of a given transmission, which is why it is widely used in online banking and other confidential transactions today. Nonetheless, when it comes to people's day-to-day communication and interactions across media environments, encryption is far from being a mass phenomenon. It requires the use of specific services and precautions on the side of the users to avoid accidentally disclosing their true identity. So, this article is not trying to argue that cryptography is the single best or only tool to counter surveillance. All the same, creating, supporting and maintaining alternative infrastructures that enable more secure and private communication means to establish conditions under which ideas can be expressed, exchanged and circulated in new ways. The examples of Tor and XMPP also underline the notion that hacking is best conceptualized as critical, creative, reflective and subversive use of technology that allows creating new meanings. In other words, the hacker organization's practices related to technology demonstrate a constructive way of countering surveillance. By doing this, the CCC is part of a global network of activists that enable a large variety of people to act with and through more secure MTI.

To expand on this line of thought, it is also interesting to note that CCC's engagement in relation to encryption and anonymizing services is double-sided. On the one hand, members use alternative technologies and infrastructures for inward-oriented communication. Since many activities—like the above-mentioned Federal Trojan hack—need to be coordinated and take place "in secrecy", the Club cannot rely on commercial platforms or other readily accessible services. From this perspective, privacy is fundamental for the Club to practice their political activities. On the other hand, the CCC brings its idea of free and secure communication to life through developing, supporting and maintaining the mentioned alternatives for the larger public. Tor and XMPP enable people to exercise anonymity and to handle data flows about themselves. Surveillance might indeed be "structurally asymmetrical" (Andrejevic & Gates, 2014, p. 192) as it is generally available only to actors with access to and control over data collection, data analysis, and database management. All the same, as the case of the CCC underlines, there are efforts to consciously and purposefully advance the cause of privacy protection. Accordingly, by acting on digital self-determination and the right to informational privacy the hacker organization is co-determining the balance of privacy, security, autonomy and democratic rights. The Club acts on creating what Warren and Brandeis (1890) called a "right of privacy" and—in many ways echoing the belief of the two Boston lawyers—refuses to believe that privacy has to die for technology to flourish. As a side effect, so to say, the case study presented in this article shows the human face of technology as it explicitly demonstrates that not machines but individual and collective human actors establish and maintain particular technologies. While the over-whelming majority of contemporary media environments is set up to gather, collect and manage big data, the CCC supports, builds, maintains and uses alternative media technologies and infrastructures that are set up to respect privacy and to honor autonomy. The initiatives that Club members originate and encourage are "interstitial spaces within information processing practices" (Cohen, 2012, p. 1931) that provide "breathing room for personal boundary management" (Cohen, 2012, p. 1932) outside the realm of routine surveillance. Acting on surveillance assemblages therefore is based on critical, creative, reflective and subversive engagements with technology that allow creating new meanings.

Taken together what has been outlined so far, the Club's modes of engagement with MTI can be considered largely technical; which is to say that they require a high level of expertise (skills, knowledge and experience) related to technology *per se* (Kubitschko, 2015b). The hackers' contestation of surveillance assemblages, however, goes beyond "activism gone electronic" (Jordan & Taylor, 2004, p. 1), since CCC members also articulate their expertise related to contemporary MTI to a wide range of audiences, publics and actors. They do so by means of public gatherings, self-mediation, coverage by mainstream media outlets as well as by interacting with institutional politics. Ever since the early 1980s the CCC has organized public gatherings like the annual Chaos Communication Congress, which today attracts more than 6000 visitors. Self-mediation practices include running individual websites and personal blogs, creating radio shows and podcasts, as well as posting their views on popular online platform accounts. At the same time, mainstream media not only increasingly cover the Club's activities but also grant individual members—in particular the organization's spokespersons—access to their outlets. Articulating their expertise across media environments not only gives the CCC a voice that is heard by a large number of people, it also enables the hackers to raise awareness and spread knowledge related to surveillance and other related issues where politics and technology collide. This facet of articulation is particularly important because being able to act on a given issue first of all preconditions that one is aware of the existence and relevance of the issue at hand. Spreading awareness and knowledge, in other words, is a precondition to enable other people's engagement. In addition to interacting with different audiences and publics, the hackers also carry their standpoint to the realm of traditional centers of power through advising senior politicians, legislators and the constitutional court in Germany. At the same time, articulation also includes legal measures. In 2014, together with the International League of Human Rights, the CCC filed criminal complaints against the German Government for its violation of the right to privacy and obstruction of justice by bearing and cooperating with the electronic surveillance of German citizens by foreign secret services. As matters stand, the court proceeding is still taking place. No matter what the actual outcome will be, the complaint raised the public's attention towards governmental surveillance practices. In fact, making their voice heard in the domain of institutionalized politics and gaining recognition of mainstream media outlets are two dynamics that perpetuate each other in interesting ways.

In the case of the CCC, acting on the notion of privacy does not only refer to doing "stuff" with technology but also the ability to actively deal with both the functions and effects of technology. Put in more concrete terms, the Club is counter-acting surveillance assemblages through direct digital action—de-constructing existing technology and supporting, building, maintaining and using alternative media technologies and infrastructures—as well as publicly thematizing and problematizing the issue. By merging technically oriented operations and discursive activities, the hacker organization brings forward a twofold strategy: On the one hand, the hackers open up the possibility for people to use privacy enhancing technology, and on the other hand, the CCC spreads awareness and knowledge related to surveillance and privacy. Instead of exclusively relying on cryptography and the science of secret communication, the Club practices a form of activism that acknowledges the relevance of counter-acting surveillance assemblages on different layers. Accordingly, in addition to co-creating interstitial spaces for personal boundary management within information and communication landscapes (Cohen, 2012), the hacker organization also takes part in shaping discursive spaces that establish exchanges of knowledge, flows of information and new levels of awareness. Taken together, this demonstrates that the CCC's interventions in the domains of technology can therefore be conceptualized as interventions in social and political domains.

5. Conclusions

Following the quasi-omnipresent spread of media technologies and infrastructures, surveillance has turned into a mundane practice enacted by a wide range of entities. The approach taken in this article is not to discuss surveillance *per se*, but instead to examine how one of the world's largest (and Europe's oldest) hacker organizations is countering contemporary surveillance assemblages. To do so, I have first illuminated the correlations between online platforms, locative media and big data—three elements that have lastingly influenced the way people experience surveillance and the way surveillance is practiced. Subsequently, the article has explicated the growing intersection of governmental and private-sector efforts related to surveillance. Taking these expanding assemblages of surveillance (see Haggerty & Ericson, 2000) as a starting point of discussion, the line of argumentation followed Cohen's concept that "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship" (Cohen, 2012, p. 1905). By presenting qualitative research on the Chaos Computer Club, the article illustrates the ways in which the hacker organization is acting on "an indispensable structural feature of liberal democratic political systems" (Cohen, 2012, p. 1905). More concretely, it has made clear that counter-acting surveillance assemblages and establishing new regimes of privacy is taking place through bringing together direct digital action and different forms of articulation. That is to say, the Club deconstructs existing technology as well as supports, builds, maintains and uses alternative media technologies and infrastructures. At the same time, CCC members also spread knowledge and create awareness towards issues related to surveillance and privacy by articulating their "technical" expertise to a wide range of audiences, publics and actors. Accordingly, it is argued that hacker organizations like the CCC provide an exemplary case study for highlighting the efforts of civil society organizations to counter-act contemporary surveillance assemblages that infiltrate people's everyday-life. Following the reasoning that privacy is critical for democratic citizenship to flourish, the Club's engagement can be considered a contribution to the formation of indispensable structural features of contemporary democratic constellations.

Acknowledgments

The author would like to thank the highly valuable feedback provided by the reviewers of this article. The research presented in this article was made possible by a scholarship from Goldsmiths' Media and Communication Department and the University of Bremen's Creative Unit "Communicative Figurations" (funded within the frame of the Excellence Initiative by the German Federal and State Governments). I would also like to thank Corey Schultz at the University of Southampton for improving the readability of this article.

Conflict of Interests

The author declares no conflict of interests.

References

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3).

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence: University Press of Kansas.

Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society*, *12*(2), 185-196.

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communication & Society*, *12*(5), 639-657.

Ball, K., & Snider, L. (2013). *The surveillance-industrial complex: A political economy of surveillance*. New York: Routledge.

Barnard-Wills, D. (2012). *Surveillance and identity: Discourse, subjectivity and the state*. Aldershot: Ashgate.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance*. Cambridge: Polity.

Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, *11*(6), 985-1002.

Beniger, J. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge: Harvard University Press.

Bennett, C. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge: MIT Press.

Beyer, J., & McKelvey, F. (2015). You are not welcome among us: Pirates and the State. *International Journal of Communication*, *9*, 890-908.

Brevini, B., Hintz, A., & McCurdy, P. (2013). *Beyond WikiLeaks: Implications for the future of communications, journalism and society*. London: Palgrave Macmillan.

Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*, *14*(7), 1164-1180.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, *24*(2), 84-88.

Cohen, J. (2012). What privacy is for. *Harvard Law Review*, *126*(7), 1904-1933.

Cohen, J. (2015/forthcoming). The surveillance-innovation complex: The irony of the participatory turn. In D. Barney, G. Coleman, C. Ross, J. Sterne, & T. Tembeck (Eds.), *The participatory condition*. Minneapolis: University of Minnesota Press.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. London: Verso.

Couldry, N. (2012). *Media, society, world: Social theory and digital media practice*. Cambridge: Polity.

Couldry, N., & Turow, J. (2014). Advertising, big data and the clearance of the public realm. *International Journal of Communication*, *8*, 1710-1726.

Dean, J. (2009). *Democracy and other neoliberal fantasies: Communicative capitalism and left politics*. Durham: Duke University Press.

Derakhshan, H. (2015, July 14). The web we have to save. *Medium*. Retrieved from https://medium.com/matter/the-web-we-have-to-save-2eb1fe15a426

Fuchs, C., Boersma, K., & Albrechtslund, A. (2012). *Internet and surveillance: The challenges of web 2.0 and social media*. London: Routledge.

Gane, N., Venn, C., & Hand, M. (2007). Ubiquitous surveillance: Interview with Katherine Hayles. *Theory, Culture & Society*, *24*(7–8), 349-358.

Garfinkel, S. (2001). *Database nation: The death of privacy in the 21st century*. Cambridge, MA: O'Reilly.

Gillespie, T. (2010). The politics of "platforms". *New Media & Society*, *12*(3), 347-364.

Gomez, J. (2004). Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia. *Pacific Journalism Review*, *10*(2), 130-150.

Graham, S. (2004). *The cybercities reader*. London: Routledge.

Greenberg, A. (2012). *This machine kills secrets: How WikiLeakers, Cyberphunks, and Hacktivists aim to free the world's information*. New York: Dutton Adult.

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622.

Haggerty, K., & Ericson, R. (2006). *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Hepp, A. (2012). *Cultures of mediatization*. Cambridge: Polity.

Hjorth, L. (2013). Relocating the mobile: A case study of locative media in Seoul, South Korea. *Convergence*, *19*(2), 1-13.

Howard, P. (2015). *Pax Technica: How the Internet of things may set us free or lock us up*. New Haven: Yale University Press.

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?* New York: Routledge.

Katz, I. (2012, April 17). Tim Berners-Lee urges government to stop the snooping bill. *The Guardian*. Retrieved from theguardian.com/technology/2012/apr/17/tim-berners-lee-monitoring-internet

Koskela, H. (2000). "The gaze without eyes": Video-surveillance and the changing nature of urban space. *Progress in Human Geography*, *24*(2), 243-265.

Kubitschko, S. (2015a). Hacking politics: Civic struggles to politicize technologies. In E. Gordon & P. Mihailidis (Eds.), *The civic media reader*. Cambridge: MIT Press.

Kubitschko, S. (2015b). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence*, *21*(3), 388-402.

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (2014). Editors' introduction. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. ix–xvi). Cambridge: Cambridge University Press.

Lauer, J. (2011). Surveillance history and the history of new media: An evidential paradigm. *New Media & Society*, *14*(4), 566-582.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Philadelphia: Open University.

May, T. (1992, November 22). The crypto anarchist manifesto [Electronic mailing list message]. Retrieved from http://www.activism.net/cypherpunk/crypto-anarchy.html

Möller, J., & Mollen, A. (2014). *The NSA in the German quality press*. Paper presented at Multi-method-designs in Transnational and Transcultural Comparative Research Workshop, Bremen.

Monahan, T. (2006). *Surveillance and security: Technological politics and power in everyday life*. New York: Routledge.

Murakami, D., Ball, K., Lyon, D., Raab, C., Graham, S., & Norris, C. (2006). *A report on the surveillance society. Report for the UK Information Commissioner's Office.* Wilmslow: Surveillance Studies Network.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press.

Rosenberg, J. (1969). *The death of privacy*. New York: Random House.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York: W.W. Norton.

Schwartz, R., & Halegoua, G. (2014). The spatial self: Location-based identity performance on social media. *New Media & Society*, online first.

Temperton, J. (2015, July 15). No U-turn: David Cameron still wants to break encryption. *Wired*. Retrieved from http://www.wired.co.uk/news/archive/2015-2007/2015/cameron-ban-encryption-u-turn

Trottier, D. (2012). *Social media as surveillance: Rethinking visibility in a converging world*. Aldershot: Ashgate.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, *19*(7).

Uldam, J. (2014). Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. *New Media & Society*, online first.

Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford: Oxford University Press.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality.* New York: The New Press.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. New York: Basic Books.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75-89.

About the Author

Dr. Sebastian Kubitschko

Sebastian Kubitschko is a post-doctoral researcher at the Centre for Media, Communication and Information Research (ZeMKI), University of Bremen, where he is a member of the interdisciplinary Communicative Figurations network. His research focus is on how hacker organizations gain legitimacy and the ways they politicize contemporary technology. Sebastian holds a PhD from Goldsmiths, University of London, and is the European Editor of Arena Magazine. Together with Anne Kaun he is currently editing a volume on emerging methods in media and communication research.

Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 88-97
Doi: 10.17645/mac.v3i2.266

Article

Literacies for Surveillance: Social Network Sites and Background Investigations

Sarah Jackson Young

Department of English, Arizona State University, Tempe, AZ 85287, USA; E-Mail: smjacks4@asu.edu

Submitted: 8 April 2015 | In Revised Form: 22 June 2015 | Accepted: 23 July 2015 |
Published: 30 September 2015

Abstract

In September 2013, civilian contractor Aaron Alexis entered the Washington Navy Yard and murdered twelve people before being fatally shot by police. This incident, together with an incident three months earlier involving Edward Snowden, caused the U.S. government to critically examine their background investigation (BI) process; because both Snowden and Alexis had supposedly slipped through the cracks of their investigations, there must be some flaw in the BI procedure. The U.S. Committee on Oversight and Reform concluded that rules forbidding "background checkers from looking at the Internet or social media when performing checks" was one of the main factors contributing to defective BIs (Report, 2014). Since the report's release, the Director of National Intelligence has been debating and trialing whether information from the Internet should be used to form a data double for BIs (Kopp, 2014; Rockwell, 2014). Using this conversation as a discussion catalyst, I argue that due to the nature of the data double, if the United States were to adopt the use of social networking sites (SNSs) for security clearance purposes, neglecting to take into account basic principles of SNSs into the process of BIs may lead to misinformation and unfavorable adjudication. Ultimately, being literate about the social practices involved in SNSs and surveillance would benefit not only investigators, but anyone, including academics, looking at individuals in online spaces.

Keywords

background investigations; data double; literacies; sorting; surveillance

Issue

This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction

In 2013 after government contractors Edward Snowden and Aaron Alexis used their security clearances for purposes other than the government intended (Snowden leaked classified information and Alexis gained access to a secured facility where he then murdered twelve people), the U.S. government began to question the BI process that allowed both to be in cleared positions with access to protected information and protected places. According to a letter in November 2013 from U.S. Representative Darrell Issa, Chairman of the Committee on Oversight and Government Reform, Issa demanded, due to the problems caused by Alexis and Snowden, that the agency which conducted both of the BIs, the U.S. Office of Personnel Management (OPM) should release "detailed information about the policies and process" that Alexis and Snowden went through for their clearances (Issa, 2013, p. 1). Issa believed that by examining these processes, problems with BI would emerge.

While Snowden became a catalyst for the procedure review, Alexis' case became the model of what was wrong with the entire process. After months of investigation on these practices, in February 2014, the Committee came out with a report detailing three major flaws to the BI procedure. The first was lack of cooperation from police departments. The second was lack of continuous monitoring. Third, "[r]egulations prohibit background checkers from looking at the Internet or social media when performing checks" (Report, 2014). Each "flaw" reportedly contributed to, at least in Alexis' case, "slipping through the cracks." Even though this report was a case study of Alexis, is has become a guideline for what needs to be changed in the industry.

While each of these points merits additional conversation, the third point is the focus of this paper. The full House report called "Slipping Through the Cracks: How the D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process" details that OPM's Handbook has not changed since July 2007, and since that time, Google searches and social media sites such as Twitter and Facebook have become very popular. According to the committee, "These three social media and search sites, among others, contain a treasure trove of information about their users" (H. Rep., 2014, p. 36). The report goes on to say how unfortunate it is that the handbook denies investigators the ability to use the Internet for anything other than minimal information such as looking up business addresses. The document concludes that "[t]his restrictive policy keeps nearly every piece of information on a Subject's social networking site outside the reach of security clearance investigators" (p. 36), and the report recommends updated policies which "would allow federal investigators to pull information about Subjects from of [sic] these and other websites" (p. 37). Merton Miller, the Associate Director of OPM, addressed these criticisms and confirmed the agency was already working to include use of the Internet in investigations, and that appropriate legislation would iron out access to the sites and verification of the information from the sites. The rationalization is that the sites would assist in forming "a more complete picture of the Subjects under consideration for a security clearance than currently exists today" (p. 38). This complete picture, or data double, would then be sorted for the purpose of granting or denying the clearance.

Incorporating social media into a BI may seem like a logical step in keeping up with a candidate considering the private sector often utilizes some type of social media review (i.e., "Social Intelligence Corp," n.d.). Not everyone agrees with this move though, and the government's use of this information is being debated between agencies. While some government officials such as those in the U.S. House's Committee on Oversight and Government Reform think information from SNSs is a treasure trove of information, others, such as Miller are more cautious about the validity of that information. This tension highlights an interesting area of study for those interested in issues of surveillance. Largely overlooked in surveillance studies, the area of BIs provide a vital illustration for understanding the intersection of surveillance, social media, and policies that could pave the way for additional uses of personal information. By examining the nature of data doubles and SNSs, this paper concludes that social media literacy is needed when incorporating SNS data into a data double for the purpose of a security clearance. Otherwise, information presented in a data double may be misinterpreted to the detriment of the subject under investigation.

2. Data Doubles and the BI

For the BI, the sorting of applicants into either a clearance grant or denial comes down to a data double. According to Haggerty and Ericson (2000), data doubles are essentially deconstructed bodies which are fragmented into components and reassembled to form a kind of virtual self to be used for surveillance. Haggerty and Ericson comment that the observed body is "[f]irst it is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows. The result is a decorporealized body, a 'data double' of pure virtuality" (p. 611). The body thus gets taken apart and analyzed in different places by different methods; it is removed from its original setting, and it is then brought together again and a newly-formed way. It is no longer the body of the individual, but it contains information from that original body. The rhetoric of the data double is described in power, among many things, as shifting (Lyon, 2007, p. 114), moving freely into new representations (Gilliom & Monahan, 2013, p. 22), circulating and unknown (Haggerty & Ericson, 2000, p. 613), transcendent, and "comprised of pure information" (p. 614). The data double becomes another version of the self which is fluidly reassembled in different ways by different people in different places for different purposes.

By creating this investigative file, the U.S. government is basically creating their version of a data double for surveillance purposes. Currently, in order to obtain a security clearance or be deemed suitable for a specially designated position of public trust or national security, an individual must first go through the BI process. Applicants either fill out the December 2010 SF-86 form which is used to conduct BIs for national security positions (U.S. Office of Personnel Management [USOPM] "Questionnaire for National Security Positions," n.d.), or applicants fill out the September 1995 SF-85P form which is used for public trust positions (U.S. General Services Administration, n.d.). As of 2015, ninety percent of the US government's background investigations are conducted by OPM, and these investigations span over one hundred federal agencies (USOPM, "Background Investigations," n.d.).

The content of the SF-86 form asks for basic identifiers such as name, date of birth, place of birth, social security number, telephone numbers and email address (USOPM, "Questionnaire for National Security Positions," n.d.). Candidates also must fill out additional basic background information for the past ten years such as their residences, education and employment histories. The form also asks for foreign travel and foreign associates, criminal history, credit information, mental health history, any history of alcohol or drug abuse, and associations with questionable organizations. The SF-85P asks similar, but fewer questions and often reduces the time accounted for to seven years (USOPM "Questionnaire for Public Trust Positions," n.d.). According to the SF-86 and SF-85P forms, the information gathered from these forms serve a basis for the subsequent background investigation, and the results of this investigation are used for adjudication purposes. The information obtained from the investigation process is then compiled in this investigative file, and the assembled content is intended to provide "the full universe of information the adjudicators can consider" (H. Rep., 2014, p. 8). This report is forwarded to an adjudicator who reviews only this investigative file. These investigations are adjudicated based, among many things, on criteria such as the applicant's reliability, trustworthiness, allegiance to the U.S., foreign influence and preference, sexual behavior, conduct, financial considerations, alcohol and drug use, psychological conditions, and use of information technology systems ("Adjudicative Guidelines," 2006). Other points of consideration are criminal conduct, security violations, outside activities, and misuse of information technology systems (H. Rep., 1999).

In terms of the investigative file for the BI, the U.S. government makes their version of the data double when they compile an investigative file on an applicant. The data double would be an assemblage of all the information gathered on the individual for the purpose of the investigation. As mentioned in the directions of the SF-85P or SF-86, this data double could be comprised of any of the required information for the form such as name, date or place of birth, residence or employment history, personal interview, and any subsequent information obtained to verify this information.

If SNS were included, details that a user would provide on a SNS align nicely with the SF-86 and SF-85P forms, especially regarding name, date or birth, city of residence, and educational background. Many of these elements are asked for and/or volunteered by SNS users. All of these elements could be compared, corroborated, or found to be discrepant from information provided by a subject during an investigation. Other things that might be identified on a SNS are things like underage drinking (H. Rep., 2014) or friendship with foreign nationals (Kopp, 2014). The SNS could be, as the U.S. House of Representatives stated, "a treasure trove of information about their users" (H. Rep., 2014, p. 36). All this information could flow into one investigative file as part of a data double.

The nature of the adjudication process though, complicates the use of a data double in a BI. To explain, as shown, the adjudicator would not be talking to the subject of the investigation him/herself; the adjudicator would just be looking at this investigative file or data double. This would be an abstracted, decorporealized body there to be sorted. Depending on what the data double was made up of, the adjudicator would decide on position suitability, and this person would be sorted into a clearance granted or denied position. This is problematic though because as Lyon (2007) reports, many times an individual may feel that their data double "does not accurately represent them" (p. 90). An individual may feel that what shows up in investigative file may not fully represent, or misrepresents, their life.

A quick example of the potential problems that the data double could lead to in the BI is alluded to in a summary report of the flaws involved in Aaron Alexis' investigation. In a press release, the U.S. Committee on Oversight and Government Reform pointed out that over 450 law enforcement departments did not fully cooperate with the OPM BI process (Report, 2014). In Alexis' case, the Seattle Police Department did not fully divulge information about a gun-related arrest, and there was also limited information provided about an anger-fueled black-out. While Alexis may have been able to get his clearance based on this lack of information, it may not go this way for others. For instance, if a clearance candidate was arrested by a law enforcement agency that did not cooperate with the investigative process, then incomplete information may only be available to an adjudicator, and the adjudicator may not be able to see that the arrest information was only a minor charge or that charges were dismissed. This incomplete information may in fact hurt an applicant. While an individual may be able to defend and respond to questions from an adjudicator about the charge, a decorporalized data double cannot answer back.

The danger of misinformation is especially true for SNSs, and adding SNSs to the BI process could offer further complications. While the above police report may have some semblance of facts, due to the nature of SNSs, information gleaned from these sites may be even less-reliable than an incomplete police report. People don't necessarily create SNSs with the intended purpose of having the government surveil them or look at the data they have posted. Users often expect to be watched, but it is most often the thought of social surveillance, or the use of social media to see what friends, family, and acquaintances are up to (Marwick, 2012), which guides their paradigm of observation. As a result of this, users don't always just report the truth or facts, and sometimes information is posted just to be entertaining. Due to the tone of the site, some users can be encouraged or feel comfortable posting information that isn't necessarily true in order to match the tone of other site interactions. For instance, according to boyd and Ellison (2008), "The extent to which portraits are authentic or playful varies across both sites; both social and technological forces shape these practices" (p. 220). Donath and boyd (2004) provide the example of a law professor on Orkut who stated his career skills were "small appliance repair" and his career interests were "large appliance repair" (p.75). In this case, this playful post didn't seem to be problematic or purposefully deceptive, but an outsider without really knowing the Subject may misinterpret the information as a falsehood if it didn't match up with other information. Misinterpretations like this may end up as a permanent record though, in one's investigative file, on the way to adjudication, and because data doubles cannot talk back, the usefulness and consequences of using this information may be detrimental to the subject of investigation. If one didn't list "appliance repair" in an employment section, they may appear dishonest. This example then brings up the importance of having some type of basic understanding, or literacy, of the practices involved in SNSs. While knowing these practices cannot verify information, they can provide an interpretive foundation for those that incorporate SNSs in to BIs.

3. SNS Literacy

According to Brian Street (1984), literacy is "shorthand for the social practices and conceptions of reading and writing" (p. 1). Knobel and Lankshear (2008) also add that literacies are "socially recognized ways of generating, communicating and negotiating meaning content" (p. 255). Implicit in these definitions is that literacy is not just reading and writing, and literacy is not just mastering a skill set or competencies. Being literate assumes that one knows the social practices that one engages in while reading and writing. Not taking into account the practices assumes literacy is neutral and not affected by situation; once someone learns to read and write, this skill will translate across every platform and situation. This is not the case though, as even a reader switching between a fiction and non-fiction text would have to understand the assumptions or practices each genre carries. Readers come to realize that fiction books are often meant to entertain rather than inform. A more robust and thorough understanding of literacy then calls for an expanded model which draws on not just skills but on the social practices and assumptions surrounding skills and spaces—all of which vary with context.

Taking information from SNSs at face value and incorporating this information in BIs/data doubles without any type of discretion or filtering process would be an example of failing to understand literacies for SNSs in BIs. Because SNSs are involved in social practices, one must be literate in the ways different assumptions alter and shape the content of SNSs. As previously discussed, an outsider looking at a SNS for the purposes other than social surveillance would already be reading SNSs out of context, and not understanding the sites' practices would further complicate any claims of objectivity. The following literacies could be used as guides for those analyzing SNSs for the purpose of BIs or any other type of analysis of SNSs. Understanding each of these literacies would be essential for the federal government or outside researchers when considering including SNS information into permanent records.

The example of Chelsea (then Bradley) Manning's Facebook page will be helpful to understand the application of these principles to SNS and BIs. Chelsea Manning was convicted in July 2013 of giving classified documents to Wikileaks. PBS's *Frontline* published an annotated version of Manning's Facebook page from the opening of his account in July 2007 to its conclusion in June 2010 ("Bradley Manning's Facebook Page," 2011). Other than Manning and Manning's ex-boyfriend Tyler Watkins, the site blurs out those that comment and post on the page. All posts listed are also those authored only by Manning with the exception of the final post on June 5, 2010 which is a post from Manning's aunt, posted under Manning's name, to let his Facebook friends know that he has been arrested. Although these posts have been annotated, what is left provides more than enough information for a case study analysis. Manning will be referred to as "he" throughout this analysis because Manning was Bradley at the time of the postings.

4. SNS Literacy and Manning

The first literacy that would be crucial to have would be functional literacy. Functional literacy of SNSs would provide a basic foundation of what a SNS even is. Selber (2004) describes functional literacy as imagining technology as a tool and participants as users. Functional literacy has often been described as mastering techniques, neutral and decontextualized out of the social sphere it exists in. A user that can maneuver around and be competent with a computer begins to be functionally computer literate. This idea is often seen in late 1990's national programs to get students ready for business in the 21st century. For instance, Cynthia L. Selfe (1999) shows that Clinton and Gore's 1996 Technology Literacy Challenge was essentially about teaching students skills on how to use a computer. A student would be literate in technology once they became competent and learned a set of finite skills. Lankshear and Knobel (2008) use the related term "standardized operational definition" (p. 3) and add this concept centers around the idea that one is digitally literate by acquiring proficiencies which may include tasks, performances, and demonstrations of skills. It involves skills like using a computer, understanding its components, and navigating the Internet. For SNSs, functional literacy could involve understanding how sites are set up and the platform limitations of them such as Twitter's 140 character limitations (while other sites such as Facebook are without these constraints).

boyd and Ellison (2008) also identified three other functional characteristics of SNSs which aren't specific to one platform and tend to permeate the overall purpose of SNSs. The first fundamental element is that SNSs are online forums which individuals can create online presences (private or semi-private) within the constraints of a defined system. Second, SNSs organize and present a list of other users on the site which the user either knows or may have a connection with. Third, more than just aggregating a group of connections, SNSs also let users look at the profiles of these connected individuals. For a SNS review, each of these characteristics would help frame the overall analysis. The sites are not necessarily geared towards a strict recounting of life events; they are often forums to discuss thoughts with connections (public or private) or to view other associations.

An investigator who was functionally literate of a SNS would need to understand the basic functions of social media or the basic components of what makes up a SNS. While this may be the most basic of literacies, being able to understand the overall site fundamentals would be an important skill for several reasons. First, functional literacy would help an investigator understand the privacy controls of the site. Investigators, depending on what restrictions are placed on access to a SNS, would want to know if they are able to actually view a page or if they would need additional access due to technological restrictions on the access to the site. They would have also need to understand if they would have access to private messages or if they are obligated to only see public information. Functional literacy of the friends on SNSs would entail understanding the ways that someone else is allowed to provide content by posting on another's page. If one is friends with another, the friends may be allowed to submit messages on someone else's page, and this may vary across platforms. For instance, photos shared and tagged through Twitter or Instagram can be shared differently or than those shared through Facebook. It would also mean being concerned with access to the individual's friend lists. If an investigator has access to one's SNS, does that mean they are able or should be encouraged to look through the list of friends? What would be the limits of looking at related pages? And, are those friends scrutinized too? Functional literacy would help set boundaries on obtaining information.

In Manning's case, Manning set up this Facebook page according to Facebook's constraints. Investigators would have wanted to understand that when Manning set up his page, only certain elements can go on that page in certain ways. For instance, Manning's first post on July 22, 2007 states, "Just created a new Facebook" ("Bradley Manning's Facebook Page," 2011). Through the timeline, Manning posts numerous other general comments such as July 27, 2008's post stating, "Home today" or August 6, 2007's "back home from Lollapalooza." Each post is identified as being Manning's by having his photo and name next to it. Throughout the timeline he also posts photos of himself like December 24, 2007's photo captioned "Just Me" and URLs such as June 28, 2008's link to Bob Barr's 2008 campaign. Facebook places the individual's name and photo next to each post, and it allows content like text, photos and hyperlinks.

Also, it would need to be understood that these are Manning's public posts (or at least public to his friends), and while these messages may have been observable to some or all of Manning's connections, they may not be observable to everyone. Facebook allows users to limit the audience of posts from the broad public to specific users ("When I post something," 2015). Additionally, there is also the messenger function which allows direct messages between users or groups of users. Investigators would need to know their information limitations.

It is important too, to understand that Manning's contacts are also able to contribute to Manning's page. For instance, on February 24, 2009, a redacted individual posted "Hahahah ah I c" and May 26, 2009 another redacted individual posted, "Ditto" ("Bradley Manning's Facebook Page," 2011). While these posts are not seemingly consequential, they do highlight others can post on the site, and posts like this bring up the question of association. If someone wrote something inappropriate, would Manning have been responsible for those quotes even if he didn't agree with them if they weren't deleted? It is also worth noting that Manning's last entry, according to *Frontline*, was posted by his aunt and read, "Some of you may have heard that I have been arrested for disclosure of classified information to unauthorized persons…" This also begs the question of the authenticity of any of the posts; while it may be Manning's page, Manning may not have been the direct poster of the entry if someone else had access to the account.

Overall then, Manning's site shows that due to the system architecture, for an outsider to understand the content of SNSs, one such as investigator would want to know functional matters like what specific technological constraints could influence the information that is contained on the site. This would matter regarding presentation of the site, privacy of the site, and contributions to the site. While this literacy may seem the most basic of understandings, it would be important to understand these elements even begin to start to decipher the information taken from a SNS.

A second literacy is rhetorical literacy. Bizzell and Herzberg (1990) relay that one understanding of rhetoric is "the use of language, written or spoken, to inform or persuade" (p. 1). Language is thus used to produce spaces in which the orator or writer creates areas of influence. According to Rheingold (2012), those posting in SNSs such as Facebook or Google+ are such participants which "seek, adopt, appropriate, and invent ways to participate in cultural production" (2012, p. 19). This participation can be anything from making a post to remixing or recreating a popular video. For Erstad (2008), being able to participate represents a shift in society from spaces that are defined by others to places where the audience can take "available content and create something new, something not predefined" (p. 178). SNSs are places where this rhetorical production happens. Users, through the constraints of a defined system, are able to create a space of their own. Having a rhetorical literacy would then entail examining the design and evaluation of these online spaces with the idea in mind that users are producers of their environments.

Further, these users don't just produce for themselves, and rhetorical production takes place in front of spectators. On SNSs, users write in certain ways for certain perceived audiences. For SNSs, a list of friends on the site can be understood as an audience. The SNS audience serves a meaningful function because this "public display of connections" (Donath & boyd, 2004, p. 72) is essential in helping shape the content of posts. Having connections on these sites presents a public for the user (Baym & boyd, 2012). The users are no longer just interacting with an unknown audience; they are interacting with a specific public where for the most part they are aware of the groups' identities. This imagined audience further causes a user to engage in behavioral norms (boyd & Ellison, 2008), and based off the users' perceived associations, the user may adapt the message they are delivering. This awareness of a public in social media also changes how people write (Baym & boyd, 2012). When dealing with connections, a person may vary what they say due to their imagined audience of their connections (boyd & Ellison, 2008). According to Donath and boyd (2004), "Knowing that everyone they interact with knows of and can communicate with a group of their acquaintances can influence their behavior" (p. 76). Further, people adjust what they are going to say based off of their audience (Baym & boyd, 2012). When SNS users are creating their profiles and constructing their identities, "they must consider how they will be received by their intimate publics and also how the public telling of their stories might affect their loved ones" (p. 324). Because of these tailored messages, an outsider would thus want to understand the values that the site and friends have and their influence upon the user's posts. Rhetorical literacy then would entail also understanding the intended audience of a SNS.

For Manning and rhetorical literacy, Manning was a producer of a site in front of his audience. It was often clear that he was writing for groups of friends and family. His aunt would have been aware of his site because she posted his final message, so his aunt was among his audience. Additionally, he addressed certain groups of people on certain occasions. On December 17, 2009, Manning states, "Thanks for all the birthday wishes at my double deuces" ("Bradley Manning's Facebook Page," 2011), and two days later he wrote, "[T]hanks everyone for all the goodies. I've been getting them! Hope to write everyone." Earlier in the year on July 4, 2009, Manning put the word out that "[Bradley Manning] needs 4th of July plan for D.C. Call me." On December 24, 2008, he "wishes you all a Merry Christmas," and on July 27, 2007, he remixed a Fergie song and asked, "[I]'d like y'all to give me some feedback." On other occasions, he singled out Starbucks coworkers such as the July 26, 2007 post addressed, "STARBUCKS PEEPS." Each of these points presents good examples of Manning addressing specific audiences. Manning did not appear to be posting random thoughts for outsiders to peruse; instead, these posts seem to be directed towards an audience that he knew personally.

While is impossible to know how Manning's posts were adapted to his audience without a direct conversation with Manning, research does show that the content of posts are influenced by site practices and the audience. Understanding Manning's audience may be a key to understanding where important information is for investigators. According to Baym (2010), "Any instance of digital language use depends on the technology, the purpose of the interaction, the norms of the group, the communication style of the speaker's social groups offline, and the idiosyncrasies of individuals" (p. 65). Thus, people write in certain ways through specific technologies for certain audiences. The postings then are not acontextual occurrences. People are aware that others are looking at them and may "feel pressured to conform to those groups' norms" (p. 81). It is thus interesting then to consider why Manning gave information to Wikileaks and also, according to *Frontline*, was reprimanded by the Army "for revealing sensitive information in video messages to his friends and family posted on YouTube" ("Bradley Manning's Facebook Page," 2011), but he did not do the same on Facebook. Audience awareness then would help signal where possibly more telling information would be divulged. For some reason, Manning was more motivated to share sensitive information with his audience on platforms other than Facebook.

A third literacy would be informational literacy. This literacy would be a key skill involved in SNS use for the BI. Informational literacy deals with being able to locate, be critical of, and use information found by digital means. Being discerning about information would determine what information was important and should be included in one's data double. For Fieldhouse and Nicholas (2008), information literacy draws on using critical thinking skills in order to decipher information from multiple, competing sources. Since SNSs often provide an overabundance of information, being able to decipher that information would be exceptionally important. Howard Rheingold's (2012) idea of crap detection fits well into this understanding of literacy. Rheingold outlines that a necessary digital literacy is to navigate through the crap that may be present on the web in order to find and use the most accurate and relevant information. This involves looking at authors, identifying publishers, and making sure information is corroborated by other sources. Rainie and Wellman (2012) touch on the same idea with their idea of skepticism literacy. They encourage that one should be able to assess the information from multiple sources in order to "weed out the media and people who have outdated, biased, incomplete, and agenda-driven or just dead-wrong ideas to pass along" (p. 274). Being cynical about the information presented then is essential then to SNS surveillance. This literacy asks the viewer (or in this case investigator) to use discretion in the information obtained on a SNSs.

For investigators involved with surveilling social media, understanding what information is valid is important. OPM's Merton Miller begins to explore the question of validity in the February Alexis report. Even though OPM was cooperating with the US House about considering whether to incorporate SNSs into the BIs, Miller himself pushed back on the incorporation of this information. Although Miller acknowledged that there may be value in looking at social media sites to identify things such as underage drinking, Miller resisted the committee's unrestrained approval of incorporating the information by making the following statement:

> Now, so what is the veracity of that information? You wrote it. You posted it. Somebody is going to have to determine the reliability of that. So that's the hard part, I think, in applying the social media role in background investigations. *It's not collecting it, it's not finding it, it's then doing the analysis, because when you run an investigation you shouldn't be incorporating information that isn't true about the subject in that investigation.* (H. Rep., 2014, pp. 37-38, emphasis in original)

This conversation and Miller's concerns raise a topic of conversation for surveillance studies to explore. While much analysis of Miller's statement can be conducted, on the surface, his comments at least start to pull back the House's larger prevailing notion that social media is a treasure trove of information about a subject.

For Manning's Facebook page, there were several things that could have been of interest for his BI. One category was the more benign but informational data. First there is the list of Manning's connections. According to the House report, this information could be used for lead purposes (H. Rep., 2014). Additionally, Manning provided basic working and living information. For instance for employments, on July 24, 2007, Manning states, "[Bradley Manning is] working at Starbucks," and on July 27, 2008 he announces, "[Bradley Manning is] working at Abercrombie & Fitch." ("Bradley Manning's Facebook Page," 2011). For residences, on December 31, 2007 Manning posts, "[Bradley Manning] is going back to Ft. Leonard Wood on Thursday," and on April 4, 2008 he states, "[I]'ve now moved on to Fort Huachuca in AZ." He also lists deployment locations such as October 29, 2009's post, "[Bradley Manning] has arrived at destination in Iraq." Since the security forms ask for employments and residences, Manning's mentioning of both could be used to corroborate information he listed on his paperwork.

Second, there was also other, possibly more derogatory information that could be found. For instance, Manning alludes to problems at employments. On November 5, 2007, Manning posts, "[Bradley Manning] is still in the Army, but suspended with injuries from Basic Training." Although it was for medical reasons, Manning still relays that he was suspended from the Army. He alludes to other employment problems, residence problems, and the feeling of living a double life in a November 17, 2008 entry. On this day, Manning posts a link to a news story and states, "I got an anonymous mention in this article. How fun!" The article links to an article on *Syracuse.com* in which an anonymous soldier (identified as Manning by *Frontline*) reveals, "I was kicked out of my home and I once lost my job," and also, due to the Army's don't ask, don't tell policy, ""I've been living a double life....I can't make a statement. I can't be caught in an act" (Her, 2008). Along these lines, many of Manning's posts openly speak of homosexual relationships which were not allowed at the Army at the time. For instance, in December 2008, Manning updated his Facebook page to announce, "Bradley is in an open relationship with Tyler Watkins." ("Bradley Manning's Facebook Page," 2011). While not problematic now, at the time it was against military policy. It bothered Manning enough that he admitted under the condition of anonymity that it caused him to feel like he was living a double life. Manning also spoke of his desired use of alcohol, and on his twenty-first birthday on December 17, 2008, he states, "[Bradley Manning] wants to get out of upstate, hit the clubs and get wasted as soon as possible!" Other statements which could be interpreted as questions of mental health were Manning's more dispirited-sounding posts. For instance, on May 5, 2010, he posted, "[Bradley Manning] is beyond frustrated with people and society at large." On April 30, 2010 he posted, "[Bradley Manning] is now left with the sinking feeling that he doesn't have anything left…" On March 10, 2009, he states, "[Bradley Manning] feels ignored by society." Each of these posts may lead some to believe Manning was feeling less than happy with life.

In order to determine the relevancy of any of these postings, some sort of established standards on information would be needed. While many of these discussed points may have been of interest to corroborate off Manning's security application or bring up questions of character, it is questionable if these would have flagged him as being a national security threat. If these elements were not on his form, he could have been flagged as being dishonest, but dishonesty regarding few things does not necessarily equate to divulging classified information. In light of functional and rhetorical literacies, too, the content of these posts are often influenced by external factors like the constraints of the site or the audience one is addressing. Just because Manning felt "frustrated with people and society at large," that doesn't meant that Manning would going to commit a heinous act; oftentimes people uses SNSs to interact with peers and receive feedback (Pempek, Yermolayeva, & Calvert, 2009) or for emotional support in times of stress (Baym, 2010). Information literacy then would be important when understanding what information is true, important and accurate and what information may be less consequential to a BI.

5. Discussion

The points at which humans make assumptions or submit "data" is an important place to analyze. In *Science in Action*, Latour (1987) encourages attention not necessarily be paid to the final product of scientific research, but instead, attention should be made in the negotiation of the process of production. Latour refers to the finished product as a black-box, a place where practices and assumptions are taken as given. Important to him instead is to look at the places where meaning-making is inscribed before the black-box is closed. Similarly, for those studying surveillance of SNSs, the practices involved in meaning- making then would be important points to examine.

As shown, when dealing with SNSs for surveillance, meaning occurs before an investigator even draws conclusions. Those posting in SNSs are engaged in practices that influence the production and outcome of their "completed," black-box profiles/investigative files/data doubles. These influences imbedded in these final products would in turn be more solidified as in investigator uses that black-box profile for their own analyses-turn-black-box investigative file. The adjudicator would further add their interpretation on the report for the determination of a clearance. Each point of scrutiny further inscribes more meaning.

This is especially true for any outsider (i.e., one who knows little background information about the Subject). Without knowing the exact meaning of posts, an outsider doing a content analysis of a SNS may not understand the practices an SNS user is engaged in. Research shows that most users are on SNSs to maintain already existing contacts (boyd & Ellison, 2008). A peer then would, for the most part, be someone that had a least a little context of who was being examined. An investigator or any other outsider, however, would be someone with little or no prior knowledge of the Subject or associations. This lack of context positions the outsider as an agent of surveillance compiling information about a Subject based on minimal, if any, perspective on the Subject other than the SNS profiles themselves. For investigations, this outsider status may even be favored; for instance, the idea of an impartial outside observer without close personal ties to a subject of investigation is usually the preferred construct. Just the term conflict of interest in law enforcement would imply an unwanted situation. In reality though, this lack of context may actually make it harder to identify the veracity of the information presented.

This lack of perspective for SNS may make achieving SNS objectivity in a BI difficult, problematic, and possibly with lasting consequences. In the context of BI's, surveillance information from SNSs could be solidified into the data double and used for sorting. This could all be based off of information that is influenced by social practice and needs to be verified and validated. The ramifications of not getting a clearance are strong, and a denial just one time may jeopardize an individual from future employment; question 25.2 on the SF-86 form asks if one has been denied a clearance (USOPM, "Questionnaire for National Security Positions," n.d.). Ultimately, then, any assumptions about SNS information based on a content analysis may be less than accurate. However, as Bowker and Star (1999) remind us, though, validity does not always matter. They state, "Equally, as good pragmatists, we know that things perceived as real are real in their consequences" (p. 53). The data double, full of investigative information, could come to be more real than the actual individual under consideration for a clearance. This is why a basic understanding of SNS literacies would be essential to even begin to use SNSs in BIs.

6. Conclusion

Civilian and government agencies use and contemplate using social media assemblages as part of their version of a data double. Looking at the nature of social media through a literacies lens shows though that many times the individual in control of a SNS profile manipulates that profile due to the constraints and norms of the communities they are part of. While this does not necessarily mean social media profiles are deceptive, it does make one question the incorporation of SNSs into the BI process which would have real consequences for those denied a position due to information on a SNS. Due to the importance of these ramifications, it would be beneficial then for those doing surveillance to have a solid understanding, or literacy, of the functional matters of what social media is comprised of, the practices it engages in, what is created and for whom, and how users and investigators shape interpretations of social media profiles. Beyond the BI, this would be important for any outsider trying to surveil SNSs for any purpose. Even academics using SNSs as spaces of study would want to be literate of these sites.

While this paper raised the need for literacies, it did not go into more specific criteria could be used. Further research into appropriate and relevant criteria would need to be conducted. The conclusions of this paper lead to a desire for more analysis of ethical considerations and of what policies should be used for examining a SNS for the purpose of the BI data double. Not understanding social network limitations ultimately may affect the sorting of profiles and eventual acceptance of employment, and as SNSs grow in popularity, these questions only become more important.

Acknowledgments

I wish to thank the anonymous reviewers for this journal and the Rhetoric, Secrecy, and Surveillance participants at the Rhetoric Society of America's summer institute for feedback on earlier versions of this paper.

Conflict of Interests

The author declares no conflict of interests.

References

Adjudicative guidelines for determining eligibility for access to classified information. (2006, February 3). Retrieved from http://www.state.gov/m/ds/clearances/60321.htm

Baym, N. (2010). *Personal connections in the digital age*. Cambridge: Polity Press.

Baym, N., & boyd, d. (2012). Socially mediated publicness: An introduction. *Journal of Broadcasting & Electronic Media, 56*(3), 320-329.

Bizzell, P., & Herzberg, B. (1990). *General introduction.* In P. Bizzell & B. Herzberg (Eds.), *The rhetorical tradition: Readings from classical times to the present* (pp. 1-15). Boston: Bedford Books of St. Martin's Press.

Bowker, G., & Star, S. (1999). *Sorting things out classification and its consequences*. Cambridge: MIT Press.

boyd, d., & Ellison, N. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*, 210-230.

Bradley Manning's Facebook page. (2011, May 24). Retrieved from http://www.pbs.org/wgbh/pages/frontline/wikileaks/manning-facebook-page

Donath, J., & boyd, d. (2004). Public displays of connection. *BT Technology Journal, 22*(4), 71-82.

Erstad, O. (2008). Trajectories of remixing: Digital literacies, media production, and schooling. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 177-202). New York: Peter Lang.

Fieldhouse, M., & Nicholas, D. (2008). Digital literacy as information savvy: The road to information literacy. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 47-72). New York: Peter Lang.

Gilliom, J., & Monahan, T. (2013). *SuperVision: An introduction to the surveillance society*. Chicago: University of Chicago.

H. Rep. (1999). *Report to the Ranking Minority Member, Committee of Armed Services. Inadequate personnel security investigations pose national security risks*. No. 05-552. Retrieved from: http://www.gao.gov/products/GAO/NSIAD-00-12

H. Rep. (2014). *Committee on Oversight and Government Reform. Slipping through the cracks: How the D.C. Navy Yard shooting exposes flaws in the federal security clearance process*. Retrieved from http://oversight.house.gov/wp-content/uploads/2014/02/Aaron-Alexis-Report-FINAL.pdf

Haggerty, K. D., & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622.

Her, P. (2008, November 17). Teen hears peoples' stories at LGBTQ rally. Retrieved from http://blog.syracuse.com/voices/2008/11/teen_hears_stories_at_lgbtq_ra.html

Issa, D. (2013, November 20). Letter to US Office of Personnel Management. Retrieved from http://oversight.house.gov/wp-content/uploads/2013/11/2013-11-20-DEI-to-Archuleta-re-in-camera-review-due-11-21-13.pdf

Knobel, M., & Lankshear, C. (2008). Digital literacy and participation in online social networking spaces. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 249-278). New York: Peter Lang.

Kopp, E. (2014, October 10). Social media could become part of security clearance process. Retrieved from http://www.federalnewsradio.com/502/3730507/Social-media-could-become-part-of-security-clearance-process

Lankshear, C., & Knobel, M. (2008). Introduction. In C. Lankshear & M. Knobel (Eds.), *Digital literacies: Concepts, policies and practices* (pp. 1-16). New York: Peter Lang.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Cambridge: Harvard University Press.

Lyon, D. (2007). *Surveillance studies: An overview.* Malden: Polity Press.

Marwick, A. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society, 9*(4), 378-393.

Pempek, T., Yermolayeva, Y., & Calvert, S. (2009). College students' social networking experiences on facebook. *Journal of Applied Developmental Psychology*, *30*, 227-238. doi:10.1016/j.appdev.2008.12.010

Rainie, L., & Wellman, B. (2012). *Networked: The new social operating system*. Cambridge: MIT Press.

Report: D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process. (2014, February 11). Retrieved from http://oversight.house.gov/release/report-d-c-navy-yard-shooting-exposes-flaws-federal-security-clearance-process

Rheingold, H. (2012). *Net smart: How to thrive online.* Cambridge: MIT Press.

Rockwell, M. (2014, November 6). Should social media affect your security clearance? Retrieved from http://fcw.com/articles/2014/11/06/odni-social-media-monitoring.aspx

Selber, S. (2004). *Multiliteracies for a digital age*. Carbondale: Southern Illinois University Press.

Selfe, C. (1999). *Technology and literacy in the twenty-first century: The importance of paying* attention. Carbondale: Southern Illinois University Press.

Social Intelligence Corp. (n.d.). Retrieved from http://www.socialintel.com

Street, B. V. (1984). *Literacy in theory and practice*. Cambridge: Cambridge UP.

U.S. General Services Administration. (n.d.). GSA Forms Library. Retrieved from http://www.gsa.gov/portal/forms/download/116382

U.S. Office of Personnel Management. (n.d.). Background Investigations. Retrieved from http://www.opm.gov/investigations/background-investigations

U.S. Office of Personnel Management. (n.d.). Questionnaire for National Security Positions. (OMB Publication No. 3206 0005). Retrieved from http://www.opm.gov/forms/pdf_fill/SF86pdf

U.S. Office of Personnel Management. (n.d.). Questionnaire for Public Trust Positions. (OMB Publication No. 3206-0191). Retrieved from http://www.opm.gov/Forms/pdf_fill/sf85p.pdf

When I post something, how do I choose who can see it? (2015). Retrieved from https://www.facebook.com/help/120939471321735

About the Author

Sarah Jackson Young

Sarah Jackson Young is a former government contractor, Teaching Associate, and fourth year PhD student in the English—Rhetoric, Composition, and Linguistics program at Arizona State University. She previously examined the Internet presence of the U.S. Department of Homeland Security during her MA, also in Rhetoric and Composition at Arizona State. Her current research interests are surveillance studies, background investigations, and use of the Internet for surveillance.

Media and Communication (ISSN: 2183-2439)

Media and Communication is an international open access journal dedicated to a wide variety of basic and applied research in communication and its related fields. It aims at providing a research forum on the social and cultural relevance of media and communication processes.

www.cogitatiopress.com/mediaandcommunication

COGITATIO