Chapter 7

Big Collusion: Corporations, Consumers, and the Digital Surveillance State

Garry Robson
Jagiellonian University, Poland

C. M. Olavarria
Université d’Avignon, France

ABSTRACT

In the post-Snowden digital surveillance era, insufficient attention has been paid to the role of corporations and consumers in the onslaught on digital privacy by the largest surveillance state – the U.S. The distinction between corporations and the government is increasingly difficult to pinpoint, and there exists an exclusive arrangement of data sharing and financial benefits that tends towards the annihilation of individual privacy. Here the role of consumers in facilitating this alliance is examined, with consideration given to the “social” performances treated as free and exploitable data-creating labor. While consumers of the digital economy often assume that everything should be free, the widespread tendency to gratify desires online inevitably leads to hidden costs and consequences. The permanent data extracted from consumer behavior helps agencies sort and profile individuals for their own agendas. This trilateral relationship of ‘Big Collusion’ seems to have gained an irreversibly anti-democratic momentum, producing new transgressions of privacy without proper consent.

INTRODUCTION

The earliest correspondence between NSA contractor and whistleblower Edward Snowden and his initial primary source, documentary filmmaker Laura Poitras, reads like something out of a work of spy fiction. One email in particular just prior to their now famed rendezvous at that hotel lobby in Hong Kong clarifies with chilling effect the very nature of unfettered global digital surveillance, which no citizen (or head of state) of any nation can escape and for which no official of the perpetrating governments has been held accountable. These words of Mr. Snowden stand alone, without rival, as a description of
the totality of undemocratic transgressions that will define this new era of mass digital surveillance by
states, and the collusive, unlawful offensives of their corporate partners:

*From now, know that every border you cross, every purchase you make, every call you dial, every cell
phone tower you pass, friend you keep, article you write, site you visit, subject line you type, and packet
you route, is in the hands of a system whose reach is unlimited but whose safeguards are not. Your
victimization by the NSA system means that you are well aware of the threat that unrestricted, secret
abilities pose for democracies. This is a story that few but you can tell (Poitras, 2014).*

Opinion regarding Snowden the man, as hero or traitor (those simplistic divisions themselves reflect-
ing simplistic and divided Anglo-American political cultures) is irrelevant, though in his own words he
claims “I am neither traitor nor hero; I’m an American” (Madison, 2014, p. 72). Ultimately it is not the
man who is on trial, but the secrets and threats he revealed. Many of those who seek to put the man on
trial over his revelations have proven to be at best state surveillance apologists, a group including cor-
porate media interests, and at worst elected officials who betray their electorates in favor of consolidat-
ing state power to protect the state and corporate enemies of democratic principles – foremost privacy,
individual autonomy and transparency.

While the greatest threats to U.S. democracy appear to be internal rather than external, as is often
claimed in justification of the ethnically questionable and unlawful policies that the state continues to
update to serve its own agenda (Shield, 2006, p. 23), the obvious reason for the implementation of those
policies is to undermine individuals or groups who question the very power they continue to consolidate:
“At this historical juncture there is a merging of violence and governance along with the systemic disin-
vestment in and breakdown of institutions and public spheres that have provided the minimal conditions
for democracy” (Giroux, 2014b, p. 41).

At one time the relationship between state and corporations in breaching the privacy of citizens was
somewhat opaque, partly because of an excess of public trust, partly because of persistent denial and
obfuscation of facts by these unchecked powers. The two were even distinguished by otherwise implicit
Orwellian terms, with private industry playing “little brother” to the state’s “big brother” (Tambini, Leon-
ardi & Marsden, 2008). Today there is no doubt, no question regarding the extent of their data-sharing
and privacy-obliterating alliance. As Price (2014) observes, “Snowden’s revelations reveal a world where
the NSA is dependent on private corporate services for the outsourced collection of data, and where the
NSA is increasingly reliant on corporate owned data farms where the storage and analysis of the data
occurs.” Following the wellsprings of big data to their source leads to the data dissemination points of
corporate communication towers and Internet Service Provider (ISP) warehouses or collection points,
with only “25 ISPs carrying around 80% of the global internet traffic” (Hathaway, 2014, p. 4). From
there big data’s origins can be traced back to the hard drives and smartphones of the average consumer;
but this process must be taken even one step further to consider the billions of terabytes being collected
and stored by the corporate-state surveillance apparatus on a daily basis (Gellman & Poitras, 2014).

It is consumers who are, inherently, the producers of the digital content that forms the third and
perhaps most important and least discussed component of Big Collusion’s digital surveillance trifecta.
The psychosocial desires of consumers motivate their digital behavior. Every search query, social media
performance, email, instant message, skype call, online purchase, application download and data packet
sent from a digital device is created from the behavioral motivations of digital consumers. But it would
Related Content

Turning Weakness into Strength: How to Learn From an IT Security Incident
www.igi-global.com/chapter/turning-weakness-into-strength/213801?camid=4v1a

The Mode of Information – Due Process of Law and Student Loans: Bills of Attainder Enter the Digital Age
www.igi-global.com/chapter/the-mode-of-information--due-process-of-law-and-student-loans/145559?camid=4v1a

Towards Intelligent Human Behavior Detection for Video Surveillance
www.igi-global.com/chapter/towards-intelligent-human-behavior-detection-for-video-surveillance/213837?camid=4v1a

Public Administrators, School Safety, and Forms of Surveillance: Ethics and Social Justice in the Surveillance of Students’ Disabilities
www.igi-global.com/chapter/public-administrators-school-safety-and-forms-of-surveillance/145571?camid=4v1a