

: Can 'Big Brother' watch us?

by Dan Power

Editor, DSSResources.com

"Big Brother" is a familiar metaphor that conjures up visions of political surveillance, political control of dissidents, totalitarian rule, and loss of individual liberty. George Orwell (1949) speculated in his novel *Nineteen Eighty-Four* about a future society where technology would help a ruling oligarchy control and dominate a pacified populace. Many have read his dystopian novel of a dehumanizing society. When the year 1984 was reached more than 30 years ago, there was a global, collective sigh of relief, we had avoided that prophecy. Big Brother's face was not haunting us on giant telescreens in Victory Square. The telescreens in our homes, offices and on the streets were not watching us and listening to us, the facts were not being edited and revised, a perpetual war did not provide the grounds for thought control and political repression. Information technology was not facilitating a totalitarian government. Computing and surveillance technologies were limited in 1984. Technology has advanced!

Apple aired its "1984" commercial during Super Bowl XVIII on January 22, 1984 as part of a marketing campaign to promote the release of the Macintosh computer. A hammer-wielding woman destroyed the video screen with the image of Big Brother. Now the "rest of us" would have computers and Big Blue would no longer control us. IBM did fall by the wayside in the race to profitably put computers in people's home and make computing a ubiquitous part of our lives. Many companies have filled the void including Facebook, Google, Samsung and Verizon.

This column reviews how technology can now facilitate the society that Orwell and others dreaded. From "big" data to video surveillance to artificial intelligence to social media, the technology pieces for centralized social control exist. Thought crimes as well as physical crimes can be identified, prevented and prosecuted. Control of these technologies remains largely decentralized, but the potential for centralized control exists. Privacy concerns should exist about **all** personally identifiable data that is collected and stored.

Privacy refers to an individual's right to determine whether, when, how, and to whom, one's personal or organizational information is collected and shared. People should expect to be free from intentional and secret surveillance without just cause. Surveillance includes watching of activities by people or video cameras. Surveillance involves monitoring of a persons behavior, activities, and movements.

The "Big Brother" metaphor focuses our attention on government data collection at all levels from local police forces with traffic cameras to the United States National Security Agency (NSA) with its very large databases. The concern about government data collection is its misuse for political

: Can 'Big Brother' watch us?

monitoring and "thought" control. Businesses also collect and mine data to improve profits and target customers, but those efforts are decentralized and uncoordinated. Conceivably government could also access that data and with metadata profile individuals.

Politicians and police authorities want more and better information. Public disputes are increasingly related to digital privacy, for example the California judge's order on February 16, 2016 that commanded Apple, Inc. to help federal investigators "extract information locked on an iPhone belonging to one of the suspected shooters in the San Bernardino, California mass murders". Traffic cameras or red light cameras are commonplace. The photoenforced.com database identifies more than 10,000 camera locations across North America. Facial recognition software is increasingly sophisticated. Also, Facebook software routinely asks if a person should be identified in a picture that is posted.

Policing technology is also becoming more sophisticated. In Fresno, California, the police use a threat-scoring system called **Beware** that analyzes a variety of data, including social media postings, to assign residents a threat level in a way similar to a credit score. The Fresno Police Department control room has 57 monitors that operators can use to zoom and pan an array of roughly 200 police cameras installed across the city and 800 more feeds from the city's schools and traffic cameras, cf., Chimurenga, 2016.

Four major technology developments have occurred since 1984 that provide the components that can be combined to implement a political/social vision similar to that described by Orwell. The remaining sections of this blog post discuss the developments and potential of "big" data, predictive analytics, social media, and artificial intelligence to create totalitarian societies. The slogan "Big Brother is watching you" from the novel defines the theme of this post and motivated its title.

Big data

We live in a digital, interconnected World. Most people cannot be anonymous on the network. Confidential documents, click strokes and digital speech can be intercepted, stored and analyzed. Perhaps it is unreasonable to expect that what people say or do is anonymous, confidential or private in contemporary society. Businesses and governments have many methods for collecting data and the cost of methods like video cameras, radio frequency identifiers (RFID) and fingerprint recognition is declining rapidly.

Some automobile drivers can get lower rates by permitting their insurers to monitor their driving behavior using a telematics device that plugs into the car's dashboard. Also, the amount of patient

data collected and stored by physicians, hospitals and insurance companies is increasing exponentially. Financial data on loans, deposits, purchases and other transactions kept by banks, financial advisors, and retailers is also increasing rapidly. One use of big data that has been documented is police departments using software from PredPol, the "Predictive Policing Company". The PredPol (<http://www.predpol.com/>) software uses crime data for a geographic area to assign probabilities for future crime events. Data is useful, very useful. We have more of it and the volume will increase because data capture and storage is inexpensive. Today we can more easily capture and analyze data in real-time, so we will do that.

Video and voice storage is a major contributor to the growth in "big" data. Video surveillance is increasing to try to reduce security threats and criminal activities. Advances in video surveillance applications such as cloud services, network cameras, analytics, as well as facial and voice recognition have increased the usefulness of video surveillance and real-time and archived data analysis. Organizations are also combining customer service records, clickstream data, IP traffic, log information, and sensor data.

The vast amounts of heterogeneous data are being combined in "data lakes". A generalized data store helps provide multiple, concurrent interpretations of related data. Teradata (3/28/2016) provided 2 example use cases, including: 1) generating improved customer churn detection models; and 2) providing for trend analytics against combinations of vast streams of machine data with consumer data.

Predictive analytics

Predictive analytics involves systematic analysis of data using quantitative and statistical models to predict and forecast results, trends and behavior patterns. Murray and Wardley (2014) identified the following major applications for predictive analytics in marketing: 1) marketing mix modeling, 2) improved lead scoring, 3) up-selling and cross-selling, 4) increase customer engagement on a Web site, 5) acquire new customers, and 6) price optimization. Credit scoring is a classic example of how effective predictive analytics can be at improving decision making. Detecting or predicting insurance fraud is also a significant application of analytics to new data sources. Utility companies are using predictive analytics to monitor energy usage and to avoid electricity outages. Also, the United States Internal Revenue Service (IRS) and many state governments use revenue collection models and analytics to improve tax collection. As a final example, predictive models have been used to help determine high-risk situations, terror threats, and crime hotspots for preventive action.

Information technologies are converging, for example Google provides cloud-computing services that include image identification, voice recognition and AI technology, including machine learning. Integrating data collection and interpretation across multiple sources and using multiple analytical

technologies is becoming easier and faster.

Social media

Web-based and mobile technology applications like Facebook can enhance human communication and create dynamic, interactive dialogues. The social data is however stored and analyzed. The most information rich social media platform is the social networking site Facebook that links individuals together by shared interests. Social media is increasing its penetration in our lives. Social media is a powerful channel for shaping opinions and a rich source of data about people and their individual likes and dislikes. Data from social media can inform business and governmental decisions. Much social media data is “publicly” available and it can be analyzed to stereotype individuals and predict behaviors. A common use of social media analytics is to assess customer sentiment to support marketing and customer service activities. Customer sentiment is a close parallel to political sentiment.

Artificial Intelligence

Thinking machines are part of the technology mix that enables monitoring and watching the actions of individuals. IBM is heavily promoting a cognitive system named Watson in television ads. A major selling point is that "IBM Watson thinks with us to help out think competitors." This claim positions IBM Watson as a business decision support system. Watson has probably not advanced to the point where this claim of "help out think competitors" is actually true, but there have been major advances in cognitive computing. In early 2011, IBM Watson was introduced on Jeopardy as the "world's most advanced 'question answering' machine, able to understand a question posed in everyday human elocution — 'natural language,' as computer scientists call it — and respond with a precise, factual answer (NY Times, 6/16/2010)." Tools like Siri and Amazon Echo with Alexa in the consumer market place show the possibility.

Implementation and Systems Integration

Computer-based analysis and decision support began impacting global society in the early 1950s. By 1995 the Web was facilitating wider deployment of analytics and decision support. Sixty years of decision support technology progress has had many impacts on what managers do, how organizations operate, how people think, and what is considered important. Today, organization decision making is linked to data from many sources and analysis of data is viewed as important. Managers want insight into customer behavior, more predictability in the supply chain and faster, more agile responses in changing, competitive situations. Analytics and decision support are

providing solutions for managers and organizations.

The technologies are converging, for example Google provides cloud-computing services that include image identification, voice recognition and AI technology, including machine learning. Analysts and decision makers can extract and analyze data in real-time and use decision support tools that were not available prior to the advent of wireless and cellular technologies. High definition remote cameras, sensors, distributed databases, statistics software, and data mining can be connected into systems and the technologies are improving. Remote distributed data gathering and decision support changes what is possible and what is expected by managers. In general, managers assume that data and analyses will be available at any time when it is needed.

The "good" news is that that despite technology advances implementation of a surveillance system that is geographically dispersed will be time consuming and costly in a large nation state using the various technologies needed for the level of control described in *Nineteen Eighty Four*. Some recent projects have been failures. For example, the \$400+ million Virtual Case File project by the SAIC Corp. was declared "unfit for use" and the \$900+ million Lockheed Martin Sentinel project was a failure. The UK National Offender Management Information System project was abandoned after a three-year delay and doubling of costs. According to Krigsman (2009), the project was supposed to create a single database allowing UK prison authorities to track and manage offenders while they are in custody and following their release. Technology development and integration is always a major challenge. Implementation of more sophisticated monitoring and prediction systems would likely start in government centers like Washington, D.C., U.S and London, UK. Moving beyond government centers and large cities would be more challenging. In some ways the police monitoring in cities like Fresno, CA, US provide prototype and test bed implementations for future systems. We often learn from our information technology project failures and mistakes.

Conclusions

Big data can mean big problems for individuals and organizations. Edward Snowden's NSA leaks demonstrate some of the problems of data privacy and security. Also, many people wrongly assume there is a right to privacy in the United States. Linder (2013) notes however that "the U. S. Constitution contains no express right to privacy." He does explore some implicit protections in the U.S. Constitution, but the framers of the U.S. Constitution did not and could not anticipate the rapidly evolving technology possibilities for collecting and analyzing data about people, their beliefs and behaviors. Organizations are collecting extensive data about individuals including customers, employees, and suppliers. More behavioral and unstructured data will be collected in the future and it will be analyzed.

We live in a crowded world struggling to cope with a growing shortage of some physical resources

: Can 'Big Brother' watch us?

by substituting information technology. What seems indisputable is that technology is enabling change and people are adopting new technologies because of how a specific technology might improve or favorably alter their lives. Managers and politicians are adopting new technologies to enhance revenues, improve operations and management control. A totalitarian superstate called Oceana is now possible. Some components of a thought control and surveillance system exist. The components can be connected and improved. In 2003, the American Civil Liberties Union (ACLU) warned in a report that "Big Brother" is no longer a fiction. Technology innovation and progress has advanced dramatically and the possible threat of what the ACLU called a "surveillance society" is now much greater.

Both American and Global society are being transformed and permanently altered by information technology. Perhaps we are creating smarter cities and a smarter planet. Businesses are investing heavily in using descriptive and predictive analytics to analyze customer and operations data to improve service, increase customer satisfaction, and increase efficiency. People can benefit from the information technology trends if data ownership and data analysis remain decentralized. The potential harm from technology developments increases the more centralized and comprehensive a national government's data collection and data storage become.

The broad question we must consider is how to put analytics, decision support and big data to use to make a positive difference in people's lives. We cannot stop the transformation that is occurring even if we desired to do so, but we can shape, restrict and potentially limit how the technology can be used, especially by government agencies. My guess is the technology transformation will accelerate, so in democratic political nation states like the United States, United Kingdom, Ireland and so many others, people must be cautious and vigilant to protect personal privacy and personal liberty. Big data, predictive analytics, social media, and artificial intelligence can be very useful or harmful or some mix of both those outcomes. We need to determine what the line is between protecting national security and preventing crime and maintaining personal and civil liberties. Information systems researchers and practitioners should **not** passively accept any use information technologies for behavioral prediction, monitoring and surveillance, or distortion of facts.

Is abandoning our communication and information technologies the only way to prevent a surveillance-driven Big Brother society? **No**, but see Rushton (2013). Understanding the potential of various information processing and surveillance technologies can help people act proactively to avoid or minimize the harmful uses of these technologies. Preventing a totalitarian police state will require vigilance by concerned citizens. Democracy requires individual rights, civil liberties, and privacy balanced with democratic, self-government, personal safety and economic opportunities.

Abuse of power and the need to protect freedom has been an ongoing problem in human society. James Madison noted in a speech at the Virginia Convention to ratify the United States Federal Constitution on June 6, 1788 that *"Since the general civilization of mankind, I believe there are more*

: Can 'Big Brother' watch us?

instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power, than by violent and sudden usurpations; but, on a candid examination of history, we shall find that turbulence, violence, and abuse of power, by the majority trampling on the rights of the minority, have produced factions and commotions, which, in republics, have, more frequently than any other cause, produced despotism. If we go over the whole history of ancient and modern republics, we shall find their destruction to have generally resulted from those causes." See James Madison <http://www.thefederalistpapers.org/>

How can we avoid a totalitarian surveillance state? Prohibit secret and general, all-encompassing surveillance and monitoring of our daily lives. Surveillance is harmful and protecting privacy is important (cf., Richards, 2013, Citron & Gray, 2013).

References

1. ABC30/KFSN Fresno (2015-07-08) Fresno (CA) Police Unveil Real Time Crime Center; Civil Rights Advocates Worry at URL <http://www.9-1-1magazine.com/PPT-Real-Time-Crime-Center-Unveiled-Fresno-CA> .
2. Appleton, R. (2015-07-07) Fresno police unveil state-of-the-art crime tracking system, The Fresno Bee at URL <http://www.fresnobee.com/news/local/crime/article26671756.html> .
3. American Civil Liberties Union (January 15, 2003) "‘Big Brother’ is No Longer a Fiction, ACLU Warns in New Report," at URL <https://www.aclu.org/news/big-brother-no-longer-fiction-aclu-warns-new-report> .
4. Chimurenga, T. (January 13, 2016) "Big Brother is having a field day in Fresno with scary surveillance technology," Daily Kos, at URL <http://www.dailykos.com/story/2016/1/13/1469470/-Big-Brother-has-lost-his-mind>.
5. Citron, D. K. and D. Gray, "Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards," Harvard Law Review, June 21, 2013 at URL <http://harvardlawreview.org/2013/06/addressing-the-harm-of-total-surveillance-a-reply-to-professor-neil-richards/>
6. Crump, C. and M. Harwood, "Big Brother is coming: Google, mass surveillance, and the rise of the 'Internet of Things'," Salon, March 26, 2014 at URL

: Can 'Big Brother' watch us?

http://www.salon.com/2014/03/26/big_brother_is_here_google_mass_surveillance_and_the_rise_of_the_internet_of_things_partner/

7. Flamm, M., "Meet the computer that can outsmart IBM's Watson," Crain's, Sept. 29, 2014 at URL <http://www.crainsnewyork.com/article/20140929/TECHNOLOGY/140929888/meet-the-computer-that-can-outsmart-ibms-watson> .

8. IBM Watson at URL <http://www.ibm.com/smarterplanet/us/en/ibmwatson/what-is-watson.html> .

9. Jeffers, D., "FBI rolling out high-tech 'Big Brother' monitoring system," PC World, Sept. 10, 2012 at URL http://www.pcworld.com/article/262071/fbi_rolling_out_hi_tech_big_brother_monitoring_system.html

10. Kaplan, A. M. and M. Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media". Business Horizons, 53 (1), 2010, pp. 59–68.

11. Krigsman, M., "UK prison IT: Massive and 'spectacular' failure," ZDNet.com, March 14, 2009 at URL <http://www.zdnet.com/blog/projectfailures/uk-prison-it-massive-and-spectacular-failure/2353>.

12. Lindner, D. "Exploring Constitutional Conflicts," 2013 at URL <http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html>

13. Murray, G. and M. Wardley (2014) The Math of Modern Marketing: How Predictive Analytics Makes Marketing More Effective, IDC White Paper at URL http://www.sap.com/bin/sapcom/en_us/downloadasset.2014-06-jun-12-15.the-math-of-modern-marketing-how-predictive-analytics-makes-marketing-more-effective-pdf.bypassReg.html.

14. Orwell, G. (1949) Nineteen Eighty-Four. A novel. London: Secker & Warburg.

15. Power, D.J., "Using 'Big Data' for analytics and decision support," Journal of Decision Systems, Volume 23, Issue 2, 2014, pages 222-228 at

<http://www.tandfonline.com/doi/full/10.1080/12460125.2014.888848>

16. Power, D.J. and G. Phillips-Wren, "Impact of Social Media and Web 2.0 on Decision-Making," *Journal of Decision Systems*, Volume 20, Issue 3, 2011, pages 249-261 at <http://www.tandfonline.com/doi/abs/10.3166/jds.20.249-261> .

17. Richards, N., "The Dangers of Surveillance," *Harvard Law Review*, May 20, 2013 at URL <http://harvardlawreview.org/2013/05/the-dangers-of-surveillance/> .

18. Rushton, K., "The only way to stop Big Brother is to give up phones and the internet - we're not going to do that," *The Telegraph*, June 13, 2013 at URL <http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/10118884/The-only-way-to-stop-Big-Brother-is-to-give-up-phones-and-the-internet-were-not-going-to-do-th-at.html>

19. Snyder, M., "14 incredibly creepy surveillance technologies that Big Brother will be using to spy on you," *Infowars*, July 10, 2012 at URL <http://www.infowars.com/14-incredibly-creepy-surveillance-technologies-that-big-brother-will-be-using-to-spy-on-you/>

20. Teradata Press Release, "Teradata Revolutionizes Enterprise Data Lake Design and Deployment," March 28, 2016 at URL <http://dssresources.com/news/4500.php>.

21. Thompson, C., "What Is I.B.M.'s Watson" June 16, 2010 at URL http://www.nytimes.com/2010/06/20/magazine/20Computer-t.html?_r=0 .

Author: Daniel Power

Last update: 2016-05-30 04:46