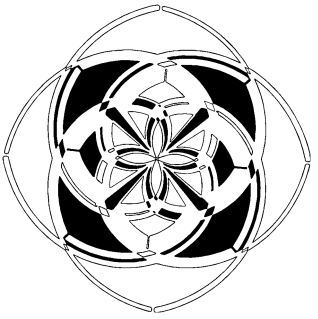
Citizen Revised

by Dagwood Engelberg

Citizen Revised

An Analysis
by
Dagwood Engelberg

Albuquerque Office
Spring Equinox, 2018



Applied Chaos Dynamics Control Association

Document E22413-G-5

Typeset in Kinnari
with Debian Linux and LibreOffice

I. Introduction

In the second decade of the 21st Century, as "Twitter Revolutions" spread across the Arab World, Western journalists sang a new verse in an old song about "the democratizing power of the Internet." As Middle Eastern demonstrators posted details of their activities to commercial social media, Western observers enthralled by the first-person, minute-by-minute updates (in English, no less) frequently credited Western technology with the protesters' ability to organize mass demonstrations effectively.[1]

After the 24-hour news cycle moved on, subsequent retaliatory government crackdowns received far less attention than the pro-democracy demonstrations.[2] The rosy rhetoric about political empowerment through social media, however, still shapes the perceptions of many Westerners.[3]

In March 2018, Tunisian authorities extended emergency police powers in force since the 2010 self-immolation of Mohamed Bouazizi prompted mass demonstrations. Iranian protests beginning with a contested 2009 election led to arrests, purges of reform-minded officials, and disappearances of journalists. As of January 2018, political unrest continues to periodically erupt in Iranian cities.

After protests in Tahrir Square, the 2009 Egyptian "Twitter Revolution" resulted in theocratic rule by the Muslim Brotherhood, followed by a military coup in 2013. Since 2015, an anti-terrorism law threatens stiff fines for journalists who publish stories contradicting official government positions. In Syria, protests bled into a civil war, and the country's autocratic president used social media to identify and round up dissidents who had organized on commercial social media.

In the United States, the Twitter-branded #Occupy movement organized popular enthusiasm around a keyword, but failed to produce much by way of a coherent critique, social agenda, or a mission-driven political organization. Elsewhere in the Greatest Democracy on Earth, the increased use of social media for political organizing has led to increased amounts of soft money in politics, foreign influence peddling among the global oligarchy, vigilante online

1 Jared Keller, "Evaluating Iran's Twitter Revolution." *The Atlantic* (18 June 2010).

2 Ivan Krastev, "Why Did the 'Twitter Revolutions' Fail?" *New York Times* (11 November 2015).

3 Maeve Shearlaw, "Egypt five years on: was it ever a 'social media revolution'?" *The Guardian* (25 January 2016).

disinformation campaigns of "fake news," and an unpopular, erratic, and potentially dangerous presidency characterized by some type of undiagnosed personality disorder.

Bound up with the distinctly anti-social character of so much commercial social media, a largely unregulated electronic surveillance apparatus gleans valuable behavior science data from fact and lie alike. Built and maintained by industry in collusion with government, every year this active monitoring system penetrates deeper into millions of homes, hearts, minds, jobs, medical records, travel patterns, dating behaviors, and political perceptions.

To dismiss these concerns because one "has nothing to hide" misses one key aspect of the risks this attitude involves: since nobody knows exactly what different organizations collect, how they analyze it, or how long they store it, one can't really know whether one ought to have something to hide. Put another way: if you believe laws exist for a reason, then when the government shows a pattern of disregarding the law, you have sufficient grounds to be concerned whether or not you consider yourself a criminal.

It would seem that in many cases, "the democratizing power of the Internet" encourages copious personal expression, but ultimately renders greater benefit to those distant television personalities who service a pathological attraction to the exercise of raw power. To explain the persistence of the Internet's "democratizing" rhetoric, one might point to the social media echo chamber as easily as the vast resources available to industrial media corporations to push this perspective. Whatever the cause, there remain largely unexamined consequences for Western cultures and participatory political institutions, which appear under duress both in Europe and the US.

II. Rhetoric and Reality

Interviewed by Gary Wolf in a February 1996 *Wired* feature, Apple co-founder Steve Jobs opined that "the web is an incredible democratizer."[4] As the Internet began to permeate daily life in the West, Jobs predicted that "once you're in this web-augmented space, you're going to see that democratization takes place." His use of the word "democratization" reflects a populist mix of techno-evangelism

4 Gary Wolf, "Steve Jobs: The Next Insanely Great Thing." *Wired*, vol. 4.02, p. 102 (February 1996).

promising liberation from traditional capitalist hierarchies,[5] combined with an outdated image of 19th Century entrepreneurship long since eradicated by industrial cartels and mass management techniques.[6]

Steve Jobs was hardly alone in his optimism. After The Wall came down and the Cold War ended, the interests of industrial monopolists like Bill Gates and corporate behemoths like IBM converged upon a consensus with the changing political order. By the time Bill Clinton was elected in 1992, his team had already developed a fairly detailed policy framework to encourage the widespread adoption of networked computing devices.

A 1992 *New York Times* column by William Broad, for example, included a much-parodied turn of phrase attributed to Vice President Elect Al Gore. Mr. Gore promised to create an "information superhighway" that would function as a "catalyst to cultural and industrial progress" by linking "computers in Government, universities, industry and libraries."[7] After the election, Vice President Gore took the lead with the Clinton Administration's technology policy team and began working on measures relating to intellectual property, data storage, cryptography, government partnerships with industry, and public network infrastructure.

---

5 For example: Kevin Kelly, "Wealth If You Want It." *Wired*, vol. 4.11, p. 193 (November 1996). An interview with Dallas Federal Reserve Bank economist W. Michael Cox makes a variety of "evangelizing" claims about computer technology and its implications. The introduction contains: "Cox's America is a land rich in opportunity. Work hard, get an education, settle down, learn something about computers ... and good things will follow." From the interview: "We're always having some kind of technological progress. Right now it's the computer chip, which, I think, is the second most revolutionary invention of mankind. The first would be electricity." Or: "you have to pay more attention to the development of your human capital. And part of that is really learning how to operate a computer... I'm trying to provide a formula that works for everyone. Anything could work for those who make 800 on the math portion of their SATs." Or: "That's the most dangerous myth of all — that the rich are getting richer, the poor are getting poorer, and most of us are going nowhere. This suggests that society should turn against the rich ... the people most of us aspire to be."

6 C. Wright Mills, *The Power Elite* (1956), ch. 11, sec. 4: "Nineteenth-century America was a middle-class society, in which numerous small and relatively equally empowered organizations flourished. Within this balancing society there was an economy in which the small entrepreneur was central, a policy in which formal division of authority was an operative fact, and a political economy in which political and economic orders were quite autonomous... But the society in which we now live consists of an economy in which the small entrepreneurs have been replaced in key areas by a handful of centralized corporations, of a polity in which the division of authority has become imbalanced... and, finally, the new society is clearly a political economy in which political and economic affairs are intricately and deeply joined together."

7 William J. Broad, "Clinton to Promote High Technology, With Gore in Charge." *New York Times* (10 November, 1992).

By the end of 1995, personal computers running Microsoft Windows were becoming as common as microwave ovens. Almost overnight, Windows 95 teleported computers from the world of nerds and into offices and homes, giving millions of people their first taste of interactive CD-ROM publishing and, soon, to Internet service providers like America Online and CompuServe. After Netscape (maker of the Navigator web browser that later became Mozilla FireFox) became a publicly-traded company in 1995, "the dot-com bubble" began to inflate, thrusting technology reporting into the pre-blogger nightly news. Every night, familiar and trustworthy network news anchors told America how computer technology was making the world more wired, more democratic, more cool, and more money.

During all the excitement about stock markets, video games, free speech and information superhighways, the Clinton Administration advocated for both increasing electronic communications and increasing the government's ability to monitor electronic communications. At the time, strong encryption software was considered a munition subject to export controls, and the DES national encryption standard may well have been deliberately weakened by the National Institute of Standards and Technology under pressure from the National Security Agency in the 1970's.[8]

Partly due to increasing electronic commerce and digital communications use by people like lawyers, CEO's, and bankers, the Clinton Administration pushed for a technology called the Clipper Chip *in lieu* of de-regulating encryption. The Clipper Chip would be installed in digital telephones and computers to ensure private communications, while keeping an extra set of password keys "in escrow" so that any communication could still be monitored by authorities. While the Clipper Chip proved overwhelmingly unpopular and ultimately insecure, in 1994 President Clinton signed the Communications Assistance for Law Enforcement Act, or, CALEA, which required telecommunications carriers to provide digital wiretapping capabilities for law enforcement and intelligence agencies. During the first decade of the 21st Century, the last remaining telecommunications carriers were brought into CALEA compliance.

Somehow, the government policies bound up with the technologies fueling "the democratizing power of the Internet" rapidly begin to resemble something the East German Stasi might have devised. Further, the "revolutionary" ability of individuals to organize on social media has a poor track record when it comes to

8 Danielle Kehl, Andi Wilson, and Kevin Bankston, "Doomed to Repeat History? Lessons fro the Crypto Wars of the 1990's." Open Technology Institute (June 2015).

actually changing the socio-political order. Beyond surveillance by authorities, online commerce increasingly monitors and records the speech and preferences of individuals as well, often with little oversight or regulation — and sometimes in collusion with government agencies. In the words of security researcher Bruce Schneier: surveillance is the business model of the Internet.[9] There is a disconnect between the rhetoric and reality of the Internet's power, and this in turn masks profound implications not just for commerce and activism, but for the nature of citizenship itself.

III. Surveillance as a Philosophy of Control

While one may hear occasional jokes about getting put on "the list" because of a Google search, in East Germany during the Cold War, few individuals would have found much humor in such sentiments. In addition to paid employees, the East German secret police maintained power through the use of a network of nearly 175,000 "voluntary" informants.[10] Close to a third of East Germans were closely monitored by subsequent ranks of state functionaries. Combining intimate knowledge of the population with the application of psychological pressure, the Stasi stifled political dissent while minimizing the application of direct physical brutality.

Surveillance isn't a "passive" phenomenon that amounts to a potential threat if placed in the wrong hands: surveillance is control. Surveillance as an active form of social control was the basis of philosopher Jeremy Bentham's 1787 treatise *Panopticon*. Describing a novel prison design, the ideas in *Panopticon* were also described as "applicable to any sort of establishment, in which persons of any description are to be kept under inspection." The idea was simple: inmates would be kept in cells along the circumference of a circular prison, while a central guard tower with small openings would both conceal the guards and allow them to observe any cell at any time.

Bentham's *Panopticon* model of surveillance and population management, applied to an entire state, formed the basis of the surveillance society depicted in George Orwell's 1949 novel *1984*. While attempting to hide from electronic surveillance by "Big Brother," Orwell's protagonist Winston Smith speculated about how

9 Fahmida Y. Rashid, "Surveillance is the Business Model of the Internet: Bruce Schneier." *Security Week* (9 April 2014).

10 Peter Wensierski, "East German Snitching Went Far Beyond Domestic Surveillance." *Spiegel Online* (10 July 2015).

the secret police worked: "There was ... no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to ... You had to live — did live, from habit that became instinct — in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."

French philosopher Michel Foucault addressed the psychological consequences of this type of surveillance system in his 1975 book *Discipline and Punish*: "Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power ... the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they are themselves the bearers."

The East German police state used a vast network of terrified informants to manage the citizenry: the American system encourages individuals to volunteer information about themselves and their friends to corporations like FaceBook, Twitter, Tinder, and therefore, to the National Security Agency as well. With access to all content posted to the public Internet, with access to communications metadata under CALEA, with access to raw network traffic and sophisticated analytic techniques like "deep packet inspection,"[11] and through the use of warrants or administrative subpoenas under the USA PATRIOT Act, records requests sent to FaceBook or Verizon can affect hundreds or thousands of people at a time. Under these conditions, the American public effectively volunteers to do the legwork required for its own mass surveillance,[12] with citizens "caught up in a power situation of which they are themselves the bearers."

---

11 Michael Kassner, "Deep Packet Inspection: What You Need to Know." *TechRepublic* (27 July 2008).

12 Dan Geer, "We Are All Intelligence Officers Now." RSA Conference, San Francisco (28 February 2014): "Even Julian Assange, in his book _Cypherpunks_, said 'Individual targeting is not the threat.' It is about a culture where personal data is increasingly public data, and assembled en masse... There are 3+ billion new photos online each month, so even if you've never uploaded photos of yourself someone else has. And tagged them. In other words, you can personally opt out, but that doesn't mean that other folks around you haven't effectively countermanded your intent. In short, we are becoming a society of informants. In short, I have nowhere to hide from you."

IV. Domestic Surveillance in the United States

One needn't speculate about what politicized intelligence agencies might do if they were to systematically target US citizens individually because of who they associate with socially. In 1975, Senator Frank Church headed up the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. In some 14 published volumes, the Church Committee documented cooperation between intelligence agencies and telecommunications carriers under a decades-old program called Operation SHAMROCK. Clocking in at nearly one thousand pages, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, provides an extensive account of how intelligence agencies worked to control the nation's political discourse by monitoring, intimidating, manipulating and harassing citizens asserting political views opposing official policies.

Over the course of many years, the FBI used techniques that were "adopted wholesale from wartime counterintelligence, and ranged from the trivial (mailing reprints of *Reader's Digest* articles to college administrators) to the degrading (sending anonymous poison-pen letters intended to break up marriages) and the dangerous (encouraging gang warfare and falsely labeling members of a violent group as police informers)." To obtain detailed personal information about targets, the FBI cooperated with the CIA through a mail-opening program called HTLINGUAL. Using HTLINGUAL, the FBI intercepted roughly 28 million letters both legally and by theft, the exterior of nearly 3 million letters were photographed, and nearly a quarter million were opened and inspected.

Abuses of intelligence capabilities documented in *Book III* frequently concern operations carried out by the FBI under a program called COINTELPRO, including: attempts to disrupt the Women's Liberation Movement;[13] attempts to destroy the Socialist Worker's Party and the Black Panther Party; attempts to discredit Dr. Martin Luther King, Jr.; breaking and entering; efforts to prevent speaking, teaching, and publishing; disseminating derogatory information to family, friends and associates; nuisance drug arrests; the creation of a new Ku Klux Klan chapter;[14] surveillance of a serviceman's

13 Church Committee, *Book III*, ch. II, sec. B contains a number of case studies covering several political groups.

14 Church Committee, *Book III*, ch. II, sec. B, Case no. 11, Ku Klux Klan: "As part of its COINTEL Program of using covert action against domestic groups, the FBI assisted an informant in the Ku Klux Klan in his efforts to set-up a new state-wide Klan

counseling center, anti-war groups, and underground newspapers; illegal mail openings; anonymous cartoons, photographs, and letters meant to ridicule activists; cultivating "cooperative press contacts;" collusion between the NSA, CIA, and FBI;[15] collaboration with college campuses to identify dissidents and activists;[16] and maintenance of files on Americans.

Following these and other disclosures about the scale and severity of the abuses, Congress passed the Foreign Intelligence Surveillance Act of 1977 to provide intelligence agencies rapid approval for urgent surveillance requests, while providing additional oversight and limiting the ability of intelligence agencies to collect information on US citizens. The law also created the Foreign Intelligence Surveillance Court to issue rulings on surveillance law.[17]

After the events of September 11, 2001, the Foreign Intelligence Surveillance Act was repeatedly amended, changing key parts of the law. Along with amendments to FISA, laws like the USA PATRIOT Act and the USA Freedom Act modified many basic legal mechanisms separating intelligence agencies from domestic targets. Additionally, PATRIOT introduced new legal mechanisms for obtaining information through administrative subpoenas like national security letters.[18] National security letters allow authorities to compel the disclosure of information without judicial oversight, while also

---

organization independent of the regular Klan... The Committee's investigation revealed that this tactic risked increasing violence and racial tension... The FBI informant in the rival Klan group also called for violence against blacks."

15 Church Committee, *Book III*, "CIA Intelligence Collection About Americans: Chaos And The Office Of Security," pp. 679-783.

16 Church Committee, *Book III*, ch. II, sec. B, for example: "7. New Left" and "8. New Left Directives." Certain targeted groups like the US Communist Party became blanket excuses for broad targeting: "The CPUSA program targeted not only Party members but also sponsors of the National Committee to Abolish the House Un-American Activities Committee and civil rights leaders allegedly under Communist influence or simply not 'anti-Communist.' The Socialist Workers Party program included non-SWP sponsors of antiwar demonstrations which were cosponsored by the SWP or the Young Socialist Alliance, its youth group. The Black Nationalist program targeted a range of organizations from the Panthers to SNCC to the peaceful Southern Christian Leadership Conference, and included most black student groups. New Left targets ranged from the SDS to the Interuniversity Committee for Debate on Foreign Policy, from all of Antioch College ('vanguard of the New Left') to the New Mexico Free University and other 'alternate' schools, and from underground newspapers to students protesting university censorship of a student publication by carrying signs with four-letter words on them."

17 Elizabeth Goitein and Faiza Patel, "What Went Wrong with the FISA Court?" Brennan Center for Justice at New York University School of Law (2015).

18 American Civil Liberties Union, "National Security Letters." Retrived from https://www.aclu.org/other/national-security-letters

sanctioning the recipient of the letter against disclosing the existence of the letter. When an administrative subpoena is issued to an Internet service provider seeking, for example, records on an IP address used by multiple subscribers, the legal bar can be quite low for obtaining certain types of non-content data like phone numbers or email addresses, depending on the record requested.

A 2013 ruling by the Foreign Intelligence Surveillance Court, for example, legalized certain types of domestic dragnet surveillance that were formerly prohibited. Some of the easier records to acquire involve transactional data, or, "metadata," which means information about a communication: what numbers are pushed on a telephone pad, what cell tower a phone communicates with, when an email was sent, what its subject header was, who sent it and who received it.

While metadata doesn't reveal the content of a communication, it is in important ways more valuable. When two people speak on the phone, the connection may be poor, the two people may speak in slang or cant or jargon, in oblique reference to the offline world, in personal idiosyncrasies or deceptively or unintelligibly. Metadata is more valuable because it never lies and is always objective and empirical. While metadata isn't content, it may still "leak" content in different ways: if one types one's banking pin into a phone, those digital "signals" are also metadata subject to disclosure under a "pen register" request.

Metadata's significance is evident in a secret 2013 FISA court ruling, to the effect that "it is necessary to obtain the bulk collection [sic] of a telephone company's metadata to determine ... connections between known and unknown international terrorist operatives."[19] The FISA court thereby authorized multiple intelligence agencies to conduct the mass recording and analysis of domestic communications that the court was in part established to prevent. The secret FISA court laid the groundwork for this change in a 2006 ruling leaked by Edward Snowden, essentially by redefining the meaning of the word "relevant" used in the surveillance laws passed by Congress.[20]

---

19 Goitein and Patel, ch. III, pt. B, sec. 1: "In its 2013 decision, the FISA Court ruled that all Americans' phone records were relevant to authorized international terrorism investigations... It concluded, in short, that because collecting irrelevant data was necessary to identify relevant data, the irrelevant data could thereby be deemed relevant."

20 Goitein and Patel, ch. III, pt. B, sec. 1: "Snowden's disclosures not only confirmed the continuing existence of the bulk collection program; it revealed that the administration, concerned about continuing its now public surveillance activities without statutory cover, had enlisted the FISA Court's help to operate this program under FISA. The FISA Court's decision in 2006 to allow mass collection of this data was based on an expansive new interpretation of the concept of 'relevance.' This interpretation made its

In June 2013, when former intelligence contractor Edward Snowden leaked classified documents to journalists detailing American surveillance programs, President Obama appeared on national talkshows to clarify what intelligence agencies were and were not doing. While President Obama told Americans that "nobody is listening to your telephone calls," the NSA was simultaneously building a data center in Utah to the tune of roughly one million square feet, or, about half the square footage of the Empire State Building.

Today, programs like HTLINGUAL and SHAMROCK go by names like PRISM, Stormbrew, Oakstar and Blarney. What the intelligence agencies once did illegally is now mandated by laws like the PATRIOT Act, modified by secret legal interpretations under the Foreign Intelligence Surveillance Court.[21] An NSA program called FOXACID automatically hacks computers targeted with XKeyScore, and a number of subprograms under the moniker QUANTUM manipulate DNS requests, impersonate host servers, manipulate data in transit, redirect page requests, target TOR users, and control IRC bots.[22]

A unit in England's GCHQ called JTRIG has access to the NSA's QUANTUM network,[23] and leaked internal documents describe an organization that, like an online global COINTELPRO, "targets a range of individual, group and state actors across the globe who pose criminal, security and defense threats. JTRIG staff use a range of techniques to, for example, discredit, disrupt, delay, deny, degrade, and deter."[24] Software tools like BURLESQUE were designed to spoof text messages, SUNBLOCK can "deny functionality to send/receive email or view material online," the Sigint Forensics

---

first appearance in 2004, when the court approved the NSA's bulk collection of Internet metadata under a different statutory provision that also requires relevance."

21 Charlie Savage, "Democratic Senators Issue Strong Warning About Use of the Patriot Act." *New York Times* (16 March, 2012).

22 Bruce Schneier, "How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID" (7 October 2013). Retrieved from: https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

23 Glenn Greenwald, "How Covert Agents Infiltrate The Internet To Manipulate, Deceive, And Destroy Reputations." *The Intercept* (24 February 2014). Retrieved from: https://theintercept.com/2014/02/24/jtrig-manipulation

24 Mandeep K. Dhami, PhD, "Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations." Human Systems Group, Information Management Department, Dstl (10 March 2011), "Executive Summary." Marked TOP SECRET, partially redacted.

Laboratory "was developed within NSA," and ANGRY PIRATE can "permanently disable a target's account on their computer."[25]

The long-standing intelligence sharing agreements between the US and UK[26] raise the possibility that the global surveillance system may be used to circumvent domestic laws against foreign intelligence agencies monitoring domestic targets.[27] In the 1960's, when the FBI was using intelligence from other agencies to target activists and dissidents, the CIA was using a series of front organizations like the Human Ecology Fund to provide cover by "crowdsourcing" behavior science research, with a special emphasis on human stress responses.[28] The forms of psychological harassment characteristic of many COINTELPRO operations resemble JTRIG tactics, and would appear to have been put online, streamlined, and partially automated.

Senator Church expressed his personal concerns about electronic surveillance in the 1970's: "If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology."[29]

---

25 Leaked document, partially redacted internal *GCWiki* entry titled "JTRIG tools and techniques (Redirected from JTRIG CITD — Covert Internet Technical Development)." Page marked "last modified on 5 July 2012" and "accessed 19,597 times." Page is taken from a system allowing classifications up to "TOP SECRET STRAP1 COMINT."

26 Jason Hanna, "What is the Five Eyes intelligence pact?" CNN (26 May 2017). Retrieved from https://www.cnn.com/2017/05/25/world/uk-us-five-eyes-intelligence-explainer/index.html

27 Edward Snowden, testimony to European Parliament (2014). Retrieved from http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf

28 David H. Price, "Buying a Piece of Anthropology, Part II: The CIA and Our Tortured Past." *Anthropology Today*, vol. 23, no. 5 (October 2007): "Kubark's reliance on citations from HEF-funded research, and testimony at the 1977 Senate hearings stating that MK-Ultra research was used to develop interrogation and resistance methods, demonstrate that HEF research was incorporated (US Senate 1977)... With isolation and stress having become the magic bullets for effective coercive interrogation, it was in the context of this shift away from drugs and equipment that Human Ecology sponsored ... stress research."

29 Quoted in James Bamford, "They Know Much More than You Think." *The New York Review of Books* (15 August 2013).

In *The Art of War*, Sun Tzu advises: "Attack when they are unprepared, make your move when they do not expect it."[30] A later commentary by Meng Shi further clarified the strategic purpose behind Sun Tzu's advice: "The most efficient of movements is the one that is unexpected; the best of plans is the one that is unknown." If opposition activists in the United States or elsewhere plan to organize on a wiretap, they begin their enterprise by surrendering their most valuable strategic advantage: the element of surprise. In this case, the convenience of organizing online carries distinct disadvantages — and even risks.

V. Anonymity and Citizenship

Modern ideas of citizenship are in many ways rooted in the concept of anonymity, and evolved alongside the historical development of cities as legal entities. Before Europe's Middle Ages, cities were primarily centers of administration and defense, rather than autonomous economic and political organizations with their own distinct laws, courts, and political institutions.[31]

European feudal society emerged out of the Roman Empire's collapse as rural populations coalesced around manorial estates for security. The manor originated as a plot of land granted to a Roman military commander. These estates developed legally sanctioned customs controlled by a hereditary noble, who owned the land to which serfs were tied by local law as well as for reasons of subsistence, rent to the lord, and monarchical fiat. The peasantry were the productive force of the land — fought over for centuries — who in the Middle Ages lived in extended clan networks. Because manorial custom kept these families tied to the same estate for generations, outsiders were easy to identify and regarded suspiciously. There was no social mobility, no life apart from the estate.[32]

Centuries after the Roman Empire's collapse disrupted trade between northern Europe and the Mediterranean's European, Asiatic,

30 Sun Tzu, *Art of War*, ch. I: "Strategic Assessments."

31 Henri Pirenne, *Medieval Cities* (1925), ch. III: "It is therefore a safe conclusion that the period which opened the Carolingian era knew cities neither in the social sense, nor in the economic sense, nor in the legal sense of that word."

32 Erich Fromm, *Escape from Freedom* (1941), ch. II: "In having a distinct, unchangeable, and unquestionable place in the social world from the moment of birth ... a person was identical with his role in society; he was a peasant, an artisan, a knight, and not *an individual* who *happened* to have this occupation. The social order was conceived as a natural order..."

and Semitic cultures, trade eventually resumed. As fine textiles from Flanders began to attract foreign buyers, the region began to see increasing urbanization, industry, and division of labor. Along with this, the emerging mercantile classes imported labor and attracted entrepreneurs from elsewhere seeking opportunity. Just before the Renaissance began to transform the artistic, scientific, philosophical, religious, and political outlook of Europe, individuals began to leave the feudal estates to which their families had been tied for generations.[33]

Seeking labor in cities as emerging centers of trade, individuals arrived at ramshackle developments surrounding fortified encampments called burgs, on land controlled by overlapping jurisdictions of crown, clergy, and nobility.[34] Terms like "burg" and "burgher" and "urban" and "suburban" all derive from a common root. While the defensive burg eventually diminished in importance, the sub-burg commercial activity surrounding these fortifications attracted labor from surrounding estates.[35]

As the areas surrounding these Medieval military encampments developed into cities as semi-autonomous legal, social, and commercial entities, individuals flooded in, seeking to liberate themselves from the estates and manorial customs to which they had been bound for so long. When enterprising serfs showed up in cities claiming free status, there were no members of their extended clan or manorial estates to deny their claim. After one year of residence, these anonymous individuals from nowhere were granted the legal status of citizen.[36]

---

33 Pirenne, ch. VI: "the origins of city populations should be sought not in the older population of the early fortresses, but in the immigrant population which trade brought to them ... Evidently it was not composed exclusively of those wide-traveled merchants ... it must have comprised, besides them, a more or less important number of men engaged in the unloading and the transporting of merchandise, in the rigging and the equipping of the boats, in the manufacture of carts, casks, chests or, in a word, all the necessary accessories for carrying on business. As a result, men from the whole surrounding territory were drawn to the nascent city in search of a profession..."

34 Pirenne, ch. VI: "the same man was dependent at the same time on several tribunals, according to whether it was a question of debts, of crimes, or simply the possession of land."

35 Pirenne, ch. VI: "In the history of the development of cities, the commercial suburb was considerably more important than the feudal burg. It was the suburb that was the active element, and ... therein lies the explanation of that renewal of municipal life which was merely the consequence of the economic revival."

36 Pirenne, ch. VII: "The disturbances which followed the assassination of Count Charles the Good, in 1127, permitted the burghers to realize in full their political program. The charter granted to [the town of] St. Omer in 1127 may be considered as the point of departure of the political program of the burghers of Flanders. It recognized the city as

Where formal concepts of citizenship intersect with anonymity, privacy, and surveillance, it is worth making some distinctions frequently overlooked in the popular discourse. Although terms like anonymity and privacy are often used interchangeably, each term actually identifies a distinct concept. In this context, "anonymous" means "impossible to identify" whereas "private" means "impossible to observe."

If somebody enters a café and pays for a cup of coffee in cash, that interaction is anonymous insofar as there is nothing about either the money exchanged or the coffee served that uniquely identifies either individual involved in the transaction. At the same time, that transaction is not private insofar as it occurs in a public place, potentially in plain view of other patrons. Conversely, if somebody goes to their regular physician for a checkup, there is little anonymous about that interaction: the physician ideally knows the patient in intimate detail. Yet, when one sees one's regular physician, that visit is hopefully kept private insofar as others should not be able to observe or deduce the visit's substantive content.

Just as anonymity became an important legal, political, and social tool for serfs who sought freedom through citizenship, anonymity was used tactically by colonial America's politically organized revolutionary bourgeoisie. In Revolutionary times, opposition to British rule was famously galvanized by Thomas Paine with his popular pamphlet *Common Sense*, originally published anonymously. One of the most detailed records of the public debates surrounding the ratification of the US Constitution can be found in the *Federalist Papers*, a collection of essays anonymously co-authored by Alexander Hamilton, John Jay, and James Madison under the pen-name "Publius."

The way the Framers thought about anonymity and rule of law fit within a distinct Western political tradition. John Locke, the political philosopher who inspired Thomas Jefferson's phrase "Life, Liberty, and the Pursuit of Happiness," held that the commonwealth is "to govern by promulgated established laws, not to be varied in particular cases, but to have one rule for rich and poor, for the favourite at

---

a distinct legal territory, provided with a special law common to all inhabitants ... Freedom, of old, used to be the monopoly of a privileged class. By means of the cities it again took its place in society as a natural attribute of every citizen. Hereafter, it was enough to reside on city soil to acquire it. Every serf who had lived for a year on and a day within the city limits had it by definite right: the stature of limitations abolished all rights which his lord had exercised over his person and chattels. Birth meant little."

Court, and the countryman at plough."[37] Formal equality before the law means that the law regards citizens irrespective of their individual qualities: neither wealth, status, social circle, sex nor race ought to affect how the government applies the law with a given citizen.

The idea of formal equality before the law requires a sort of anonymous, abstract, featureless individual. Economist Friedrich Hayek noted the importance of political anonymity in his 1944 book *Road to Serfdom*, in drawing a distinction between substantive equality and equality of opportunity: "A necessary, and only apparently paradoxical, result ... is that formal equality before the law is in conflict, and in fact, incompatible with any activity of the government deliberately aiming at material or substantive equality of different people ... To produce the same result for different people, it is necessary to treat them differently." Hayek is the grandfather of the modern libertarian movement, though his basic argument in favor of freedom was not anti-government, but in favor of laws based on general principles, rather than aimed at specific groups of people in order to achieve specific outcomes.

In Hayek's view, once the government acts with intent towards specific groups of people, the government ceases to be a tool of "the people" while individuals become an instrument of the government. Hayek was willing to accept a degree of inequality so long as all individuals were treated the same by the law. His argument favored public communications infrastructure, public banking, and public health care,[38] and opposed coercion whether it came from the public or the private sector.

To apply the same laws to different citizens in different ways based on an individual's personal qualities violates the principle of formal equality before the law. Hayek elaborates on this

---

37 John Locke, *Second Treatise on Civil Government* (1690), ch XI, paragraph 142.

38 Friedrich Hayek, *Road to Serfdom* (1944). Hayek believed in markets but opposed "dogmatic" laissez-faire policies. See, for example, ch. III: "The function of a competition not only requires adequate organization of certain institutions like money, markets, and channels of information — some of which can never be adequately provided by private enterprise — but it depends, above all, on the existence of an appropriate legal system, a legal system designed both to preserve competition and to make it operate as beneficially as possible. It is by no means sufficient that the law should recognize the principle of private property and freedom of contract." Also, ch. IX: "there can be no doubt that some minimum of food, shelter, and clothing, sufficient to preserve health and the capacity to work, can be assured to everybody... Nor is there any reason why the state should not assist the individuals in providing for those common hazards of life against which, because of their uncertainty, few individuals make adequate provision ... where, in short, we deal with genuinely insurable risks — the case for the state's helping to organize a comprehensive system of social insurance is very strong."

circumstance: "Where the precise effects of government policy on particular people are known, where the government aims directly at such particular effects, it cannot help knowing these effects, and therefore it cannot be impartial." To treat all people the same, formal equality before the law requires that the government address its policies towards people in their generic role as anonymous citizens, rather than single out specific people in terms of their identities as individuals or groups.

VI. Redefining Citizenship

When major media outlets cover surveillance issues, the threat of "warrantless surveillance" is typically framed within the scope of the 4th Amendment to the US Constitution. While the 4th Amendment protections against arbitrary "search and seizure" may indeed present a central problem posed by modern global surveillance, limiting the discourse on surveillance to 4th Amendment protections glosses over the fact that the 4th Amendment does not explicitly guarantee privacy, and it sidelines some other very troubling ways that Constitutional protections are undermined.

Violations of the 4th Amendment may be easiest to apprehend intuitively, but multiple legal mechanisms exist to justify a range of rights violations. Each of these different legal mechanisms carries implications for long-standing laws and traditions, with the cumulative effect that many of the "privileges and immunities"[39] enjoyed by citizens have been cast aside in favor of a new extra-legal regime.

In October 2001, President Bush issued a secret directive titled "Presidential Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism within the United States,"[40] which directed the NSA to spy on US soil under a program called Stellar Wind. The legal rationale

39 The 14th Amendment, ratified in 1870, promises that "No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property without due process of law; nor deny any person within its jurisdiction the equal protection of the laws." Some of this language was carried over from the Articles of Confederation, and represents the codification of intervening common law; for example, Article IV: "the free inhabitants of each of these States, paupers, vagabonds, and fugitives from justice excepted, shall be entitled to all the privileges and immunities of free citizens in the several states..."

40 Offices of the Inspectors General, *Report on the President's Surveillance Program* (2009), "Authorization of The President's Program," p. 7. Between 2001 and 2006, President Bush issued 43 authorizations, each slightly different and some still classified.

changed over time, and the first authorization was the only one to rely on a 4th Amendment "probable cause" standard.[41]

The second version of the authorization was signed just one month later, changing "probable cause" to "reasonable grounds to believe." The fourth authorization was issued in March 2004, and it redefined the term "acquire" to mean the querying of stored data, rather than the actual recording of a private communication. The fourth version also provided retroactive approval for previous operations carried out under the new definition of "acquire."

Along with the Presidential Authorizations, other key changes in surveillance laws were enacted under PATRIOT. Specifically, PATRIOT modified the criterion for FISA surveillance such that foreign intelligence no longer need be "the purpose" of collection, but rather, "a significant purpose."[42] Alongside this change, Congress authorized intelligence agencies to consult with law enforcement, creating a situation where intelligence can be collected about American citizens absent probable cause, provided foreign intelligence collection is a secondary aim.

Congress amended FISA in 2008, enacting provisions which, among other things, stripped states of the authority to investigate the role of telecommunications carriers in federal surveillance programs. Another provision granted telecommunications carriers retroactive immunity for complicity in illegal surveillance. US District Chief Judge Vaughn Walker, in dismissing the Hepting-Jewel case against the NSA, described the FISA amendment as including "a provision for the benefit of telecommunications companies that allowed the United States to invoke a newly-created immunity and thus seek dismissal of cases brought against telecommunications companies."[43]

While Congressional acts granting retroactive immunity seem to violate Article I, Section 9 Constitutional prohibitions against *ex post facto*[44] legislation, most case law regarding *ex post facto* laws pertain to making actions illegal retroactively, rather than retroactively legal, providing courts little precedent to guide interpretations of these provisions. Furthermore, ordinary citizens have little recourse to the courts over this issue due to the doctrine of "sovereign immunity"[45]

---

41 Offices of the Inspectors General, Appendix B, "The Presidential Authorizations."

42 Goitein and Patel, ch. II, pt. B, sec. 2.

43 Jewel-Hepting dismissal, Judge Vaughn Walker presiding. Case M:06-cv-01791-VRW, Document 703, Filed 01/21/10.

44 "Affecting things past."

and the judicially-created "states secrets" privilege[46] protecting surveillance-related documents.

A partially-declassified 2009 report by the Inspectors General of several federal agencies found that: "in stages between 2004 and 2007, NSA ceased ... collection activities under Presidential authorization and resumed them under four separate court orders issued in accordance with the Foreign Intelligence Surveillance Act of 1978 as amended (FISA)." The FISA court — created after Frank Church investigated surveillance abuses — has the ability to issue secret rulings, meets in secret, and does not require an attorney to present an opposing view when the government seeks action.

This is not governing "by promulgated established laws," but rather, by secret decree. The changes to laws, regulations, and legal frameworks that enable the modern system of surveillance threaten to change how we regard citizenship itself — if we understand citizenship to be the product of Constitutional protections constraining the actions of Congress and the Executive. The NSA, at the operational core of these changes, was itself created by a secret executive order signed by President Truman in 1952.

Other than the National Security Act of 1959 — which mostly outlines recruitment incentives[47] — Congress has passed no laws specifically regulating the agency or explicitly defining its mission, even though the agency's budget surpasses that of the FBI or CIA.[48] Increasingly, the most basic rights of Americans are defined and re-defined at will by extra-legal intelligence agencies, appointees to secret courts, and wage-earning bureaucrats following secret executive orders, rather than the actions of democratically elected representatives in Congress.

---

45 Seegers v. Gonzales, 396 F3d 1248, 1253 (DC Cir 2005): "injuries that are shared and generalized — such as the right to have the government act in accordance with the law — are not sufficient to support standing." Cited in Jewel-Hepting dismissal.

46 The "States Secrets Privilege" was given formal recognition by the US Supreme Court in the case of United States v. Reynolds (1953), 351 U.S. 1. The case involved the widows of three Air Force contractors killed in the crash of a B-29 Superfortress while testing classified electronics equipment. Subsequently declassified documents showed the crash was likely caused by a known design flaw leading to an engine fire. See http://www.fas.org/sgp/othergov/reynoldspetapp.pdf

47 Public Law 86—36; 73 Stat. 63; approved May 29, 1959 (As Amended Through P.L. 113—126, Enacted July 7, 2014). See sec. 6: "nothing in this Act or any other law ... shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof."

48 David Burnham, "The Silent Power of the N.S.A." *New York Times* (27 March 1983).

One striking consequence of ubiquitous surveillance combined with long-term data storage is that social media maintains dossier-style records of an individual's activities, preferences, and social network over time. Because postings to social media services like FaceBook or Twitter reside on the public Internet, these platforms can be used to effectively place somebody under retroactive surveillance. Should somebody at some point arouse suspicion for whatever reason, that individual's personal history can be examined in great detail, and analyzed by sophisticated pattern-detection algorithms as if that individual had been actively monitored for years.

The possibility of retroactive surveillance raises complex issues with 5th Amendment protections against self-incrimination. These 5th Amendment protections are the basis of the Miranda Rights, or, "the right to remain silent" upon arrest. The basis of this right is that, upon arrest, one has not been charged with anything, nor evidence collected, nor witnesses called to testify; for the sake of informed consent, therefore, one is made aware that one is better off saying nothing, rather than run the risk that making some seemingly innocuous statement may later become incriminating.

In the case of "open source intelligence" gleaned from services like FaceBook or Twitter, without access to legal counsel friends may testify without being made aware of it. Incriminating photographic or video evidence may be just another click away. Should some legal activity be made illegal at a later date, the possibility that an investigation into the details of somebody's personal history may reveal incriminating statements could complicate prohibitions against retroactive *ex post facto* legislation. If, rather than a law, an Executive procedure or policy position should change, the Constitution's Article I *ex post facto* prohibition may not even be relevant.

As the legal rationale for recording electronic communications changed throughout the first decade of the 21st Century, the changing circumstances whereby intelligence was passed to law enforcement created problems for cases brought to trial. Specifically, during the pre-trial discovery process, one party may compel another to produce documents, evidence, or testimony. Government lawyers — and DEA lawyers in particular[49] — needed to find ways to avoid disclosing "sources and methods" in discovery.

---

49 Mark Cooke, "Mission Creep: The PATRIOT Act and the War on Drugs." ACLU (28 October 2011): "The Patriot Act itself has been highly controversial and is much in need of re-examination. Patriot Act powers intended to combat terrorism should not be used to wage the nation's misguided war on drugs."

Rather than risk a judge ruling key evidence inadmissible because it was produced by unclear means, government lawyers began using a technique called "parallel construction" to evade discovery obligations at trial, and, specifically to avoid disclosing certain sources of information like FISA.[50] Effectively a form of "intelligence laundering," the technique involves government lawyers "making up a fake story and an alternative investigatory trail" for trial.[51] This has unclear implications for the 6th Amendment right to a "speedy and public trial" and for the right for one "to be confronted with the witnesses against" oneself.

The 4th Amendment protections against search and seizure absent a warrant issued on probable cause are undoubtedly a vital part of the US Bill of Rights. Yet its undermining by intelligence agencies, executive orders, Congressional acts, and private telecommunications carriers are only one way in which the legal strictures outlining citizenship are being invisibly revised.

VII. A Brave New World Order

When pervasive systems of surveillance strip citizens of their anonymity, citizens are simultaneously estranged from a 700-year old Western liberalizing tradition. Arbitrary changes to the substance of citizenship conjure spectres of crown rule in the days before laborers and merchants began extracting bills of rights from kings and queens.

The qualities of anonymity that inform modern notions of citizenship are evaporating rapidly under the modern surveillance regime. These virtues of anonymity range in their impact from the social reforms initiated by modern cities and mercantilism, to 14th Amendment guarantees that "All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States." Decades later, the importance of formal equality was reaffirmed with the 19th Amendment guarantee that "The rights of the citizens of the United States to vote, shall not be denied or abridged by the United States or any State on account of sex." Pervasive surveillance changes the meaning of citizenship itself, and as such, amounts to nothing less than a form of social engineering.

---

50 Goitein and Patel, ch. V, pt. B, sec. 2.

51 Jennifer Granick, "The Surveillance State's Legalism Isn't About Morals, It's About Manipulating the Rules." *Just Security*. Author served as Director of Civil Liberties at the Stanford Center for Internet and Society (November 2014).

The 1st Amendment right "to petition the government for a redress of grievances" is of little comfort when anything one says may be used against oneself.[52] Moreover, there are no technical solutions to the problems posed by pervasive surveillance.

To organize political opposition on a wiretap is to implicitly trust that one's opponent won't abuse their superior position. To opt out means to stop placing oneself and others under surveillance for the state for convenience or for fun, to avoid novelty personality surveys that can be used to build psychological profiles. To opt out means to organize opposition in person like the labor movement, the womens' movement, and the civil rights movement. To opt out means strategically using the Internet in public places where one can blend in with strangers. To opt out is inconvenient and requires discipline.

To opt out means to understand how one is monitored: if three people meet to discuss a demonstration and all turn their phones off upon gathering to ensure privacy, they have already tipped their hat by producing a correlated event that signals they don't want to be heard together. For an intelligence agency to determine this only requires a statistical correlation with the behavior of others who also wish to avoid being observed, which can be detected automatically.

Since mobile phones are in near constant communication with multiple networks — and increasingly understand speech — a more subtle way around this privacy problem would be to find a way to obscure one's activity. In the case of a private meeting, one person may leave his or her phone at home, while the other two place their still-powered-on telephones in the refrigerator (since refrigerators are airtight and keep out sound waves, while still permitting radio signals to "phone home" uninterrupted).

To opt out means to fly below the radar because there is no getting off the grid. It may mean learning to rely on Linux operating systems[53] rather than commercial software that shares the government's passion for data collection. To preserve privacy and anonymity under pervasive surveillance requires effort, and may mean mis-representing oneself to the networked world at times.

---

52 Geer, RSA: "Demonstrating exactly the kind of good intentions with which the road to Hell is paved, we have codified rules that permit our lawmakers zero privacy, we give them zero ability to have a private moment or to speak to others without quotation, without attribution, without their game face on. In the evolutionary sense of the word 'select,' we select for people who are without expectation of authentic privacy or who jettisoned it long before they stood for office. Looking in their direction for salvation is absurd. And delusional."

53 For a good list of options see https://distrowatch.com

Dan Geer, Chief Information Security Officer for the CIA's venture capital firm In-Q-Tel, spoke at the 2014 RSA conference:

> "Misrepresentation is using disinformation to frustrate data fusion on the part of whomever it is that is watching you. Some of it can be low-tech, such as misrepresentation by paying your therapist in cash under an assumed name. Misrepresentation means arming yourself not at Walmart but in living rooms. Misrepresentation means swapping affinity cards at random with like-minded folks. Misrepresentation means keeping an inventory of misconfigured webservers to proxy through. Misrepresentation means putting a motor-generator between you and the Smart Grid. Misrepresentation means using Tor for no reason at all. Misrepresentation means hiding in plain sight when there is nowhere else to hide. Misrepresentation means having not one digital identity that you cherish, burnish, and protect, but having as many as you can. Your identity is not a question unless you work to make it be. Lest you think that this is a problem statement for the random paranoid individual alone, let me tell you that in the big-I Intelligence trade, crafting good cover is getting harder and harder and for the same reasons: misrepresentation is getting harder and harder. If I was running field operations, I would not try to fabricate a complete digital identity, I'd 'borrow' the identity of someone who had the characteristics that I needed for the case at hand."

Writing around 1920, Czech author Franz Kafka wove cultural memories of the old-world style of despotism into a short parable. Called "The Problem with Our Laws," the parable opens: "Our laws are not generally known; they are kept secret by the small group of nobles who rule us." Secret laws undermine the principle of "consent of the governed" and transform citizen-electors into subjects of naked authority.

Whether or not one believes one has anything to hide, ubiquitous surveillance changes the meaning of citizenship in dramatic ways, leaving individuals with an increasingly tenuous relationship to those "inalienable human rights" the US Constitution was drafted and amended to guarantee to all citizens.

Once the sphere of citizenship expanded to be more inclusive and participatory; now it is rapidly becoming unrecognizable.

In the West, anonymity has for centuries been used as an expedient for social, political, and economic change.

The development of citizenship -- as the concept is understood today -- is intimately connected to anonymity, both in a historical sense and in terms of political philosophy.

With the advent of modern global surveillance systems, discussions of anonymity and privacy have acquired renewed importance.

As individuals are increasingly denied anonymity and privacy, individuals lose their connection to the political traditions that produced modern citizenship.

Citizenship in the United States and elsewhere in the West is currently being re-defined without democratic input.

As the importance of citizenship in the political process diminishes, individuals are increasingly made subject to impersonal systems of control.