**Modernity & the Totalitarian Potential of New Surveillance Technologies**

**Camille Tokar**

**1. On Modernity**

One of the most fascinating and frightful truths about the Holocaust is that it was facilitated by a nation of individuals who are virtually indistinguishable from people today, in an advanced and highly modern liberal democratic society, against a group of people that were so assimilated, they were visibly, culturally, and statistically unidentifiable. The individuals who engaged in the genocidal version of anti-Semitism were not unusually sadistic, fundamentalist or fanatical.[[1]](#footnote-1) Rather, they were a civilized, gentile, educated, religious people who conscientiously embraced a revolutionary scientific ethic.

The ability to murder millions of people in such a short period of time requires a few critical ingredients: a motive, the means, and a total failure of any safeguards or limits. Hitler’s revolutionary scientific ethic provided the German *Volk* with the motive: the total annihilation of the Jewry promised redemption and regeneration of the humiliated national German spirit after the First World War. However, it was *modernity* that provided the German *Volk* with the means to accomplish genocide and it was *modern rationality* that permitted the safeguards against totalitarian politics to fail completely.

In more ways than one, the Holocaust was a uniquely modern phenomenon supported by inherently modern resources. According to Zygmunt Bauman, modernity was a necessary cause and a critical component of the Holocaust’s genocidal mission.[[2]](#footnote-2) The success of the exterminatory form of anti-Semitism depended on the *practical policies* of a *powerful centralized state* in command of a *massive bureaucratic apparatus* with access to *advanced technologies*.[[3]](#footnote-3) This modern cocktail of social control, which existed pre-Holocaust (and continues to exist today), rendered the German *Volk* extremely vulnerable to totalitarianism. When Germany went into a *state of emergency*, totalitarianism was *the* natural response and Hitler’s national socialism easily took control of every aspect of private and public life. Modern safeguards against totalitarianism, for example, the liberal institutions and the doctrine of the *Rule of Law*, completely failed to protect equality and liberty for the vulnerable groups erroneously identified as enemies of the state.

According to Kren & Rappoport, what makes the Holocaust so disturbing in hindsight is the awareness that this massive scale of violence is now “within the range of human possibility.”[[4]](#footnote-4) While this is true, the fear that ought to linger in the minds of Westerners today is that despite the fact that academics, historians, theologians and philosophers have contemplated the Holocaust *to death*, and despite the fact that late modernity continues to lay the framework for totalitarian politics, *the West* has not attempted to focus on how to, or even that it ought to, take steps to mitigate modernity’s despotic tendencies.

If the “modern barriers to violent ambition and unscrupulous power have proven ineffective,” *the West* has a serious cause for concern.[[5]](#footnote-5) This paper intends to illustrate that *the* *West* continues to be *at* *least* as vulnerable to mistaken beliefs and totalitarian politics as it was pre-Holocaust through a comparison of surveillance technologies used by the Nazis with those available today. This paper seeks to explain why *the West* remains complacent to the latent, yet draconian, potential of current surveillance practices. Finally, this paper seeks to explore the moral imperatives for the legal community in light of modernity’s genocidal tendencies.

**2. Nazi surveillance techniques**

Before any group can be targeted for marginalization and eventual extermination, they must first be identified. Thus, the fact that German Jews were among the most assimilated Jews in Europe posed a significant problem to the Nazis. Occupying Germany since the fourth century, German Jews were entrenched in German culture, professions, science, politics and the arts.[[6]](#footnote-6) Furthermore, after suffering from anti-Semitism in Europe for millennia, German Jews began to *self-identify* as German to evade persecution.[[7]](#footnote-7) Europeans equated *the Jew* with non-nationality, non-conformity, and boundary transgression; yet, discrimination did not take a genocidal form.[[8]](#footnote-8) Rather, anti-Semitics were polite, civil, and respectable.[[9]](#footnote-9) Although it was not without reservation, German Jews were tolerated and reluctantly permitted to participate in German life.

Furthermore, had genocide been contemplated before the Second World War, the German state did not even have a demographic profile of its nation accurate enough to mobilize its anti-Semites. In the eighteenth century when European states began to gather census information, the basic census was distribution-oriented and used almost exclusively to calculate the nation’s military potential.[[10]](#footnote-10) The nineteenth century censuses were notoriously inaccurate.[[11]](#footnote-11) When the Nazis took power, Germany had nothing more than a rough idea of its population and distribution. Furthermore, the level of organization required to genetically identify, rank and sort millions of people through generations of hard copy community, religious and state records littered across Germany was nonexistent. Thus, although 500,000 *orthodox* Jews could technically be statistically identified through Jewish religious community registries, approximately 300,000 *biological* Jews living in Germany were “statistically invisible in a population of about 65 million.”[[12]](#footnote-12) As Hitler’s ethic was fundamentally anchored in Social Darwinism and eugenics, exterminating only the obviously orthodox Jews was unacceptable. Hitler’s ethic required the destruction of every *biological* trace of Jewry. Predictably, the Nazi state strategically justified a dramatic expansion of “the role, function and acceptability of state surveillance” by inciting national paranoia over *warfare* and *welfare*.[[13]](#footnote-13)

Contemplating the Holocaust without modern bureaucratic apparatuses, automation, and surveillance technologies would have been futile. The identification of the Jewry alone was a lofty ambition that required an active, systematic observation of millions of people, and a “concentration of power, resources and managerial skills” that could only occur in an advanced state of modernity.[[14]](#footnote-14) On the next level, the ability to use the information gathered to socially engineer a society by transporting, tracking and murdering those identified in a mere few years was a monumental cross-indexing task that would be virtually impossible without computer technologies.[[15]](#footnote-15) Mass murder required routine bureaucratic procedures, means-end calculations, budget balancing, official authorization, universal rule application, and technology.[[16]](#footnote-16)

**i. The Racial Census**

The initial lists of Jewish names used by Nazis came from a racial census taken on June 16th, 1933 invented by the innovative *solutions* company IBM Germany. The focus of traditional census taking was reoriented from *basic head counting* to *identification*.[[17]](#footnote-17) 500,000 census takers went door-to-door with paper and pen questionnaires taking a statistical portrait of each household in Germany. Information gathered included mixed marriage status, religion, profession, residence, and nationality.[[18]](#footnote-18) The results from the census were combined with 130 years worth of birth, death and land registries, community lists, baptism records, and church authorities, in what Edwin Black coined a “profession-by-profession, city-by-city, and…block-by-block revelation of the Jewish presence.”[[19]](#footnote-19) By the May 17, 1939 Census, the Nazis had managed to register, survey, number and sort virtually every practicing Jew numerous times.[[20]](#footnote-20) 750,000 census takers went to over 31 million locations to classify 80 million citizens in the Greater Reich by ancestry.[[21]](#footnote-21) Although the manual census-taking operation was tedious, it was an unprecedentedly sophisticated, invasive and thorough method of state surveillance.

**ii. IBM’s Hollerith Punch Card and Sorting System**

IBM’s Hollerith Punch Card and Sorting System, the precursor to the first computer, exemplifies the serendipitous companionship between technology, bureaucracy and the Holocaust. In anticipation of Hitler’s *Jewish Problem*, IBM Germany custom-designed a cataloguing system to enable the Nazis to efficiently identify, sort, rate, berate, track, receive, manage, ship, starve, and dispose of the Jewry.[[22]](#footnote-22) IBM staff entered the detailed census information on millions of people into punch cards day and night at a rate of 150 cards per hour.[[23]](#footnote-23) The punch cards were then tabulated in a mechanical sorter to produce critical statistical information at a rate of 25,000 cards per hour.[[24]](#footnote-24)

Reducing humans to a series of columns and holes, the punch cards held detailed information on its subjects and rendered every aspect of public and private life available for cataloguing and analysis. Columns were assigned to nationality, race, date of birth, marital status, number of children, physical attributes, skills, sexual preferences, social status, and even *reason for departure* (hole 2 for transfer to a labour camp; hole 3 for natural death; hole 4 for execution; hole 5 for suicide, and hole 6 for *special handling*, which referred to death by gas, hanging or gunshot).[[25]](#footnote-25) The punch card system and the bureaucratic context in which it worked reduced the vulnerable groups in German society to quality-free objects that could be targeted for marginalization with the push of a button. The gathering and analysis of census and historical information to identify, characterize, ghettoize and murder millions of people was not, however, the only surveillance conducted in the Greater Reich. Private citizens, official state informants, and the Gestapo also conducted state-sanctioned surveillance with legal impunity.

**iii. The *Gestapo* and Private Informants**

The German nation quickly became an intensely self-censoring population that functioned in an atmosphere of terror, fear and paranoia. The *Gestapo*, a secret police charged with an unconstrained executive authority to work against enemies of the state, had a reputation for invasive surveillance techniques, brutal interrogation skills, and lawlessness.[[26]](#footnote-26) For example, in 1941, the Nazis passed an all-encompassing law that criminalized *friendship with Jews*.[[27]](#footnote-27) The mere existence of non-Jewish names in a Jewish woman’s address book was a sufficient ground to suspect *forbidden relations* and to commence surveillance on the *non*-Jews.[[28]](#footnote-28) Notwithstanding the *Gestapo*’s notoriety, it is critically important not to collapse the *Gestapo*’s *reputation* with its *reality*.

Historical research on the *Gestapo*’s manpower and physical resources reveals that a high degree of public collaboration and cooperation was required to enforce Nazi policies.[[29]](#footnote-29) For example, in 1937, only 22 *Gestapo* officials were responsible for surveillance and enforcement of the entire Lower Franconia’s population, which totaled 840,663 in 1939.[[30]](#footnote-30) In other words, the *Gestapo* succeeded in terrorizing the nation with a very limited number of agents. Their success was due in part to the favourable response given to informants even for completely false or baseless allegations, in part to a complete lack of legal recourse for false allegations, and in part to the fact that cooperation with the Nazis was widely publicized.[[31]](#footnote-31) According to Robert Gellately, the fact that “the patently innocent could be charged on mere suspicion or technicalities, virtually with complete legal impunity…was very often publicized by the press specialist attached to the court.”[[32]](#footnote-32) The extensive propagation of false allegations and brutal tactics induced the citizenry to believe that the *Gestapo* was omnipotent.

*Gestapo* files indicate that the most significant percentage of all surveillance cases commenced, an alarming 33%, were initiated by private citizens. Politicians, academics, federal inspectors, city officials, teachers, businessmen, bankers, pub owners, white-collar workers, housewives, working women, Catholic priests and even Jews voluntarily denounced their fellow citizens.[[33]](#footnote-33) With the exception of the moles established in the underground Communist and Socialist movements, informants acted voluntarily and free from Nazi coercion, motivated far more often by spite than loyalty to the Nazi party.[[34]](#footnote-34) Thus, not only were the private lives of German citizens saturated by totalitarian surveillance tactics, Germans from all walks of life continued to trust the state, collaborated with the *Gestapo* and became active participants in their own terrorization.

**iv. Western Rationality**

Another uniquely modern signature of the Holocaust was that rather than dismantling the Jewish community by murdering its leaders first, the Nazis appealed to the Western rationality of self-preservation to break Jewish solidarity. According to Bauman, “*the rationality of the ruled is always the weapon of the rulers.*”[[35]](#footnote-35) The Nazis converged *rationality with cooperation* to manipulate the Jews into placing self-preservation above solidarity.[[36]](#footnote-36) To induce cooperation, the Nazis strategically made distinctions among the Jews and set up a loose reward system that appeared to protect and privilege cooperative Jews. For example, Jews who had served in the military in the First World War were initially exempted from conscription into the death camps; Jewish Rabbis and elites were accorded special status; Hungarian Jews were distinguished from Polish and German Jews; and violence was not distributed randomly or without cause. Although it was a lie, marginalization was *calculated* to *appear* to be based on individual merit.

Using their own rationality against them, Jews were tricked into believing that if they cooperated they could avoid the *Jewish fate*, which apparently involved persecution, discrimination, subjugation and deportation. However, by accepting special treatment, the Jews were coerced into accepting the underlying assumption that the *Jewish fate* was legitimate in the first place.[[37]](#footnote-37) The Jews validated their own subjugation and, consequentially, their solidarity was severely weakened. Prioritizing self-preservation over solidarity, Jews humbly acquiesced with the ghetto enclosures, signed up for labour camps, forfeited property, took charge of their own resettlement, controlled order in the concentration camps, and passively walked into the gas chambers for slaughter.

By reinforcing the Jewish communal structure rather than systematically targeting it, the Nazis mobilized the Jews to their advantage. In every stage of annihilation, the Jewish elites played a crucial mediating role in facilitating their own demise. The Jewish elites supplied the Nazis with personal and financial records, effectively granting them access to Jews that would not have been exposed otherwise, they supervised transportation into and out of the ghettos and concentration camps, they distributed food, clothing and medical care within the ghettos and camps, they policed and governed the captive communities, and, they were ultimately responsible for ranking their fellow Jews for annihilation.[[38]](#footnote-38) Inside the camp walls, survival displaced solidarity, and even the pillars of the Jewish communities were induced into self-surveillance.

There is no doubt that even the rudimentary surveillance technologies employed by the Nazis played an enormous role in granting the Nazis a total monopoly over German public and private life. Every aspect of every person’s life in Germany, not only the vulnerable groups, was invaded by surveillance and open for state scrutiny. Even loyal Nazis could be subject to surveillance without cause. Even more fascinating is the fact that Germans and Jews actively participated in their own subjugation to totalitarian control, at times eagerly embracing surveillance tactics to advance their own opportunistic endeavors. Surveillance was accepted as a legitimate means to exert control in a society that had at one time been the prototype of liberal democracy. Importantly, what is missing from history is just as analytically significant as what is apparent. In the 1930s, despite the existence of well-entrenched liberal institutions, something was missing because German society failed to thwart the mass murder perpetuated by Hitler’s nightmarish totalitarian politics.

**3. Legalities**

The Holocaust was, frightfully, legal. The professions played a central role in legalizing and legitimating the Nazi party’s unbridled power to discriminate by race. Doctors perverted Darwinism to provide scientific justifications for the eugenics movement.[[39]](#footnote-39) Philosophers bolstered the scientific rationale for racism with moral arguments.[[40]](#footnote-40) Lawyers subordinated longstanding legal procedures and the rule of law to legalize the discriminatory goals of the Nazi party. Adopting a moral dissonance, the professions were willfully blind to the racist bloodlust of the Nazi party and provided the moral impetus for their totalitarian surveillance tactics.

According to Frederick DeCoste, law in the Western legal tradition is a “potentially seamless web of rules woven from the ‘*golden thread*’ of legal principle [emphasis added].”[[41]](#footnote-41) The beauty and achievement of the laws in the Western liberal *corpus juris* lies in the internal morality of its rules. While all laws are inherently logically discriminatory, laws in the Western liberal tradition adhere to a higher law, known as the *Rule of Law*. The Rule of Law holds that as law descends from the priority of persons and the primacy of private life, laws must exist *only* for the sake of persons and property and must conform to principles.[[42]](#footnote-42)

As the point of the law in the Western liberal tradition is to codify liberty, the law must instantiate rights that constrain power and minimally interfere with private life.[[43]](#footnote-43) Thus, every rule in the Western legal tradition must import a background justification that is grounded in legal equality between persons and rules of proof and process. Laws must be general, stable, and prospective in application, capable of being complied with, accessible, clear and intelligible, and rationally connected to a factual predicate that triggers their application.[[44]](#footnote-44) Aiming to endow persons with as much freedom, privacy, integrity and equality as possible, the only threshold for legal interference can be *harm*.[[45]](#footnote-45)

As the gatekeeper of the law, endowed with the authority to construct, contemplate and apply the law, lawyers must have a deep understanding of the point of law as a bridle on power and of the law’s internal morality. Naturally, lawyers that have internalized the Western legal tradition are realistic about human nature, suspicious of power, insistent on procedural correctness, and rigorously defiant of straying from the status quo. Tragically, by failing to protect liberal advocacy, legal equality, and the principles that follow from the rule of law, the lawyers under the Nazi regime left Germany defenseless to Hitler’s totalitarianism. The following examples illustrate how laws were precisely drafted to systematically marginalize vulnerable groups in Germany, and thus, how Nazi law utterly abandoned the Rule of Law.

The first wave of anti-Jewish laws in 1933 ousted Jews from professional and commercial life and legalized the expropriation of Jewish assets, business, and jobs by Germans. The *German National Recovery Act* of 1933 required German businesses to give the federal government unprecedented amounts of information, Jews were prohibited from advertising in public directories and from leasing business space, and businesses, including Jewish-owned companies, were prohibited from having Jewish employees.[[46]](#footnote-46)

The second wave of anti-Jewish laws in 1934 facilitated the creating of genetic profiles that would ultimately be used to identify the biological Jews that would be targeted for annihilation. The 1934 *Law for Simplification of the Health System*, required doctors to file detailed health forms about their patients with Health Offices, who used the information to create eugenic profiles.[[47]](#footnote-47) The 1934 *Law for the Prevention of Genetically Sick Offspring* legalized a sterilization program that targeted individuals deemed insane, retarded, epileptic, and mentally ill. Of the 84,600 cases brought to the Genetic Health Courts in 1934, 62,400 people were forcibly sterilized.[[48]](#footnote-48) The scope of the sterilization program was quickly extended to social undesirables, anti-socials, foreigners, and eventually Jews.[[49]](#footnote-49) In 1935, 88,100 genetic trails resulted in 71,700 forced sterilizations.[[50]](#footnote-50)

The *Nuremberg Laws* of 1935 advanced a legal definition of *the Jew*, allowing precise yet discretionary identification of the object for surveillance. Individuals with three or four Jewish grandparents were *full Jews*, those with two Jewish grandparents were *half Jews*, and those with one Jewish grandparent were *quarter-Jews*.[[51]](#footnote-51) Those deemed of *mixed blood* were classified as Jewish at German discretion depending on how *un-German* they appeared or behaved.[[52]](#footnote-52) If a half-Jew or quarter-Jew belonged to a Jewish religion or was married to a Jew, he or she was deemed a full Jew.[[53]](#footnote-53) *The Law for the Protection of German Blood and German Honour*, prohibited marriages and intercourse between Jews and Germans, and *The Reich Citizenship Law*, classified individuals of non-German blood as state subjects, depriving Jews of citizenship.[[54]](#footnote-54)

In the Western liberal tradition, laws that are discriminatory or ambiguous are not enforced. Yet, German lawyers purposefully drafted overly broad laws for discretionary application. The racist Nazi laws totally interfered in the private enterprise and personal integrity of its citizens without meeting the minimum threshold for interference, harm. The background justifications for the laws were logically and scientifically erroneous. The legal community subverted rules of proof and process to advance Nazi goals, to preserve professional autonomy, and to reassure non-Jews that they would continue to be a privileged class. According to Udo Reifner, as authoritarian developments that supported the Nazi fascist regime were manifested first through procedural legal changes such as “deformalization, efforts to increase efficiency, and the subordination of procedures to goals,” protecting liberal procedures are even more important to protecting democratic structures than substantive law.[[55]](#footnote-55) However genuine, misguided or opportunistic their motives may have been, the legal profession allowed the Western liberal structure of the law to erode, and with it the most precious safeguard against despotism.

**4. Post-Modern Surveillance Technology**

*In the future, everyone will have their 15 minutes of anonymity*.

– Banksy.

Surveillance capabilities in late modernity have advanced so far beyond those of Nazi Germany, they pose a latent, but *limitless* potential for draconian totalitarian tactics. With the emergence of modern, formal, highly advanced surveillance techniques, surveillance has become an increasingly one-sided, impersonal and intrusive means of identification.[[56]](#footnote-56) Surveillance is omnipresent and ubiquitous in both the public and private sectors. New technologies invade and overwhelm daily life, turning everything into an object of surveillance including biological and biometric features of the human body and ordinary everyday activities. The following examples illustrate how, as technologies and information are increasingly accessible and exchanged, the distinction between public and private objectives and objects of surveillance are becoming increasingly blurred, the consequences of which could be catastrophic.

**i. Private and Public Security Surveillance Technologies**

Security surveillance technologies are evermore omnipresent in the West. According to Kerr & Barrigar, “the space for private, unidentified, or unauthenticated activity is rapidly shrinking” as the world is overwhelmed with handheld recording devices, personal webcams, interconnected surveillance cameras, global satellite positioning systems (GPS), Radio Frequency Identification (RFID) tags, smart cards, HTTP cookies, digital rights management systems, biometric scanners, and DNA sequencers.[[57]](#footnote-57) The United Kingdom alone contains an estimated 4.2 million Closed Circuit Television (CCTV) surveillance cameras in public and private spaces.[[58]](#footnote-58)

Surveillance is conducted on persons and property. RFID Tags use radio waves to remotely track, scan and store information about the movement and properties of products.[[59]](#footnote-59) Smart cameras used to identify, locate and track suspicious behavior in private and public spaces are equipped with Face Recognition Software (FRS), Gun Shot Sensors (microphones that can attenuate to specific frequency ranges), Intelligent Passenger Surveillance technologies (that alert camera operators upon detection of suspicious behavior), and GPS locators.[[60]](#footnote-60) The *suspicious* behavior noticed by these technologies includes but is not limited to congregating, loitering, leaving unattended objects, and making loud noises.

Everyday technologies are designed to conduct surveillance on their targets and their users. For example, biometric technologies are used to create *smart* cellular phones, laptops, CCTV cameras and spaces that *learn* to recognize their users and the persons watched, know their histories, respond to their preferences, and trigger security responses in restricted spaces.[[61]](#footnote-61) Second generation biometrics, such as FRS, Backscatter and Wave Millimeter technologies, gather sensory data such as pupil dilation, iris and retinal signatures, vascular patterns, fingerprints, galvanic skin response, electrical activity of the heart and brain, and even behavioral traits such as gait, posture, facial ticks and expressions, to convert the human body into a digitized profile.[[62]](#footnote-62) The technologies are not only capable of identifying and tracking their users, they are designed to do just that.

The information and profiles collected by these technologies are often held privately in data warehouses and software. However, the data is frequently shared with or sold to other private organizations and the state in response to economic pressures, crime, biological contagion, national security, taxation, employment, accreditation, insurance and financing.[[63]](#footnote-63) Public bureaucracies accesses privately held information to secure national borders and to detect identity, contraband, weapons and even deception.[[64]](#footnote-64) Law enforcement frequently uses highly individualized *smart* cellular phones to record and track a users’ “time space path” throughout the day and to locate suspects.[[65]](#footnote-65) The use of surveillance cameras, undercover policing operations and informants by the state is accepted socially, culturally, and politically as routine and necessary.[[66]](#footnote-66) Likewise, citizens passively acquiesce to the fact that creditors, employers, insurers, and taxation authorities access their personal information to cross-check, monitor and screen them.[[67]](#footnote-67) The distinction between information that can be publicly or privately collected, held or accessed is blurred.

Post-9/11, the threat of terrorism justified expanding state access to private information and resulted in a surge of surveillance in the name of national security. Shortly after the terrorist attacks, Larry Ellison, the CEO of Oracle Corporation and the fourteenth richest person alive, offered to donate software to the US government that would enable a national identification database. To the concerned public, he simply stated: “The privacy you’re concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy.”’[[68]](#footnote-68) The *USA Patriot Act* passed in 2001 expanded the authority of immigration officials and law enforcers to conduct intrusive surveillance into the private lives of its population and to subpoena information from internet service providers, cable companies, banks and education institutions without probable cause or judicial oversight.[[69]](#footnote-69) The Department of Homeland Security (DHS) implemented a panopoly of surveillance systems in airports including x-ray baggage screening, full-body scanners, behavioral monitoring, random searches, and dataveillance systems such as race-determined *no-fly* lists that would have seemed intrusive and “dangerously nationalistic” before 9/11.[[70]](#footnote-70) As of 2010, 72 DHS Fusion Centers collect data from public *and* private CCTVs, Unmanned Aerial Vehicles, and private-sector data aggregators that hold credit information, consumer preferences, and demographic and political profiles to investigate *suspicious* individuals.[[71]](#footnote-71) The information collected from the private sector would be illegal for a government to collect independently. Yet, ubiquitous surveillance and the invasion of civil liberties has become a normal response to national security issues.

Military surveillance technologies have also proliferated to new heights. During the Second World War, military surveillance had only begun to incorporate science, accelerating the pace of weapon development and radar technology.[[72]](#footnote-72) Today, military surveillance includes continual, real time data collection using noise and heat sensors, “helicopter mounted ‘people sniffers’ that detect ammonia left by human urine”, radar, remotely guided munitions, unmanned drones, video and reconnaissance cameras, and spy aircraft.[[73]](#footnote-73) According to Kevin Haggerty, “a military cartographic frenzy” has made perpetual and highly intrusive constant surveillance of mapped caves, bunkers, pipelines and cables from the stratosphere possible.[[74]](#footnote-74)

Everything and everyone is a potential object of surveillance at all times. It is no longer merely enemies of the state that are watched by the state during times of heightened threats to security. Ubiquitous surveillance is normal and inherent in all aspects of life. All individuals are subject to identification and tracking by highly sophisticated technologies whether they are at work, at home, or at play. Even those conducting the surveillance are identified, tracked and monitored by the technologies they use. While the swift advancement of technology created a limitless potential for surveillance, the objects and objectives of surveillance were radically expanded even further with the introduction of the World Wide Web.

**ii. Cyberspace**

Most people don't want Google to answer their questions…they want Google to tell them what they should be doing next…I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time.

– Eric Schmidt, CEO of Google, on the future of Google…[[75]](#footnote-75)

Since the invention of the World Wide Web, technological innovations in Cyberspace have provided the *information economy* with a limitless impetus to conduct surveillance on consumers. Ironically, the World Wide Web was originally designed to allow *ID-free* anonymous communication. However, the interactivity of the internet has blurred the distinction between producer and consumer creating a world of “prosumerism*”* where consumers are “intimately involved” in the design, production and evaluation of products and services by divulging vast streams of data for marketers to subject to surveillance.[[76]](#footnote-76) Reflexively, consumerism has become “a proxy” for citizenship, sociability, and connectedness in modern life.[[77]](#footnote-77) Thus, today even the most mundane online activities are valuable to the market economy and subject to commodification, categorization and analysis in real-time formats that can be “captured, archived and retrieved indefinitely”.[[78]](#footnote-78) According to Kerr & Barrigar, it appears that network technologies are evolving “from architectures of freedom to architectures of control”.[[79]](#footnote-79)

For example, data mining algorithms, such as Google’s *PageRank* and HTTP cookies, are sophisticated algorithmic surveillance software programs designed to extract patterns and knowledge from mountains of historical data collected from billions of unconnected people in order to predict consumer behavior.[[80]](#footnote-80) Data scraper applications “troll through twitter feeds, blogs, social networking sites, online forums, bulletin boards, and chat rooms” in real time searching for correlations that will reveal the “emotional pulse of the internet”.[[81]](#footnote-81) These surveillance programs are generally undetectable by their objects with the exception of occasional tailored pop-up ads.[[82]](#footnote-82) The fact that they are undetected, however, does not mean that they are not collating, analyzing and selling information at a dizzying pace.

The following examples illustrate how the information from data mining algorithms is utilized. Acxiom, a US marketing-communication agency, cross-analyzes consumer data from the most prestigious automotive companies, credit card issuers, banks, telecom companies, retailers, brokerage firms, pharmaceutical manufacturers, insurance providers, lodging companies, and gaming companies to identify their client’s *precise* *target market*.[[83]](#footnote-83) eXelate, a leading targeting exchange, uses data mining algorithms to scour website registration data to collect data on the age, sex, ethnicity, marital status, profession, and consumer activities to determine who is *most vulnerable* to targeted advertising.[[84]](#footnote-84) Rapleaf *sells access to individuals* through HTTP cookies using data collected from over 900 million blogs, internet forums, and social networks, 400 million consumers, and 52 billion friend connections.[[85]](#footnote-85) Lotame *gathers, monitors and stores* over 240 billion interests, actions and attributes on social networking sites *monthly,* including what online users create, rate, like, send, share, upload, comment, edit, post, watch, use, listen to, and the recency and frequency of interests or actions.[[86]](#footnote-86) Every single online activity is an object for invasion. The data collected (most of which includes very personal information) is bought, sold and used to aggressively target consumers. However, despite the fact that the Internet has taken on this frightful Orwellian character, its users are, at best, mystified by its potential and, at worst, completely indifferent.

**iii. The Participatory Movement**

Surveillance has become so culturally integrated, even when it is recognized it is accepted as ordinary and safe. According to William Webster, the normalization of surveillance has transformed daily life into a “data-producing laboratory”.[[87]](#footnote-87) People self-disclose their personal information to access services, to travel, to open bank accounts, to use mobile phones and to make purchases. However, surveillance and self-disclosure is not merely tolerated, it is embraced. People actively participate in self-surveillance recreationally, volunteering personal information for “lateral surveillance” by family members, friends, acquaintances and colleagues.[[88]](#footnote-88) According to John McGrath, since the early twenty-first century, “letting the maximum possible number of people know our moods, our whereabouts, our opinions, our plans, and even our relationship to the afterlife has become…a social necessity.”[[89]](#footnote-89) Even people that know their online activities are monitored self-disclose detailed aspects of their personal lives. For example, people share their videos on YouTube, photographs on Flickr, professional data on Linkedin, books read on GoodReads, details of trips they have taken on Dopplr, places they have visited on Foursquare, computer screens snapshots on Snoopon.me, relationship histories on Facebook, personal profiles on MySpace, and sentiments on Twitter.

Surveillance is implicitly accepted as a legitimate means of producing security and people actively participate in conducting surveillance in their private lives. People access websites such as Fyiscreening,[[90]](#footnote-90) EmployeeScreenIQ,[[91]](#footnote-91) Catchacheat[[92]](#footnote-92) and Abika[[93]](#footnote-93) to obtain detailed dossiers of people’s web trails, cellular phone use and personal histories. People conduct surveillance on their communities through websites such as Family Watchdog,[[94]](#footnote-94) Cop Watch[[95]](#footnote-95) and Busted! Mugshots.[[96]](#footnote-96) People can even actively participate in the surveillance of the Mexico-US border online through the Texas Virtual Border Watch Program.[[97]](#footnote-97) Online companies such as Microsoft, Google and Verizon actively construct a sense of online risk to children and directly link parents to monitoring software that enables them to control their children’s internet usage.[[98]](#footnote-98) WikiLeaks, a novel website from Denmark that publishes confidential government and corporate sector documents, exemplifies a new kind of upwards surveillance by people on the state that would have been unacceptable under authoritarian regimes.[[99]](#footnote-99) The participatory movement illustrates the deep integration of surveillance in the collective rationality of Western culture.

**iv. A Word on Regulation**

Surveillance has become so normalized in Western culture, its methods and objectives remain unchallenged even when surveillance technology fails. Heightened or perfected surveillance has become the only solution to its failure. According to Mark Andrejevic, as “*All* information is potentially relevant because it helps reveal patterns and correlations,” there is “no logical endpoint” to its collection.[[100]](#footnote-100) Regulatory debates around the collection of information attempt to balance security against freedom.[[101]](#footnote-101) The polarization of security and freedom tacitly implies that the two concepts are incompatible and the regulation of surveillance technologies reflects this assumption. Consequentially, the focus of surveillance regulation prioritizes civil rights, personal autonomy, accountability, transparency or trust depending on the social context in which the privacy issues arise.[[102]](#footnote-102)

Traditionally, state searches have been restricted more stringently, while in the private sector there are far fewer restraints on the collection of personal information.[[103]](#footnote-103) In Canada, the federal Office of the Privacy Commissioner, provincial Privacy Commissioners and regulatory institutions such as the Canadian Radio-Television and Telecommunications Commission (CRTC) regulate and police surveillance and the collection of personal information. Canada’s federal Privacy Commissioner deemed that live and recorded video pictures of people can only be collected in the commercial context with informed consent if it is demonstrably necessary,[[104]](#footnote-104) and that public places should only be monitored for public safety by the state if it is demonstrably necessary.[[105]](#footnote-105) Personal information can only be collected for a valid purpose with consent or by statutory authority, it must be accessible for amendment or challenge, it must be maintained accurately and confidentially and only for a necessary length of time pursuant to the Personal Information Protection and Electronic Documents Act*[[106]](#footnote-106)* and the Privacy Act.[[107]](#footnote-107)

However, despite these guidelines, political, economic, and social opposition or indifference have permitted the functions and objects of surveillance “to creep…beyond their original rationale”.[[108]](#footnote-108) Social complacency towards ubiquitous surveillance and the tacit acceptance of its legitimacy has weaved surveillance into Western culture, ignoring the latent potential for totalitarianism. According to Kerr & Barrigar, in the face of unprecedented technological growth “anonymity is…under fire.”[[109]](#footnote-109) Anonymity is not recognized legally as a human or legal right. Legally, anonymity may be treated as “anything from a fundamental right to a fundamental non-right, depending on the subject matter.”[[110]](#footnote-110) In response to aggressively targeted advertising tactics, cyber-bullying, cyber-stalking and cyber-harassment, states are lobbying for increased regulatory control in the cyberworld, seeking to heighten the identifiability of anonymous internet users and to gain more access to privately collected and held data.[[111]](#footnote-111)

The overall effects of an intrusive surveillance regime that conflates public and private objects and objectives are difficult to predict. According to Arthur Cockfield, the surveillance regime may erode democracy by reducing state accountability, discouraging the expression of political dissent, and increasing distrust between the state and its citizens.[[112]](#footnote-112) Cockfield suggests that, in light of the blurred distinction between public and private information collection and the growing tension between security and privacy, enhanced legal protection, oversight and reporting of the collection and exchange of data is necessary.[[113]](#footnote-113) Naturally, Cockfield advances an argument in favour of subjecting the existing surveillance regime to increased surveillance.

**5. When are we now?**

Within the last decade, cultural sentiments regarding surveillance have moved from a “dystopic fantasy-fear of universal surveillance” to a “largely apathetic acceptance” to an “apparent ecstasy of engagement”.[[114]](#footnote-114) Only a few years ago, even the threat of surveillance cameras raised public suspicion. Today, people expose intimate personal information online recreationally and rarely take notice of surveillance in their daily life. In late modernity, “surveillance is now the dominant organizing practice”.[[115]](#footnote-115) Western institutions are aggressively formalizing ethically limitless and self-legitimating new surveillance technologies to more efficiently identify, scrutinize, monitor and marginalize almost every fathomable population for every fathomable reason.

While it may be unconstitutional or otherwise illegal to discriminate against persons for group membership on the grounds of *protected* traits, such as race, gender, nationality, age, or disability, not a single person escapes the expanding net of *Statistical Discrimination*. Today, virtually every single commercial or governmental interaction generates data that “enhance[s] the scope and impact of our statistical constructions.”[[116]](#footnote-116) There are, practically, no alternatives to compliance with the surveillant society that now defines the West.[[117]](#footnote-117) It is arguably impossible to fully participate in society without divulging personal information and subjecting oneself to surveillance. In Canada, it can even be *criminal* not to participate with the census.[[118]](#footnote-118) Surveillance, and the heightened transparency which accompanies it, pervades every inch of Western society. Every aspect of public and private life is perceived as a legitimate object of surveillance, leaving populations today much more vulnerable under a totalitarian regime than the German population would have been in the 1930s. Thus, the question that lingers is: Why didn’t we learn anything from the Holocaust?

While the Holocaust may have changed the course of history, it “has most certainly changed little, if anything…of our collective consciousness and self-understanding”.[[119]](#footnote-119) According to Haggerty, “surveillance, fundamentally, operates as an *idea* that draws upon some of the most entrenched and weighty traditions of Western thought”.[[120]](#footnote-120) The West is inclined to privilege the notion of surveillance because it embraces the “trope of visibility,” subconsciously believing that things that are more visible are “easier to manipulate, regulate and control”.[[121]](#footnote-121) The West’s “wholesale adoption” of surveillance as the best way to achieve social order predisposes the West to embrace new surveillance technologies and to discount or dismiss the inherent tyrannical potential of a transparent society.[[122]](#footnote-122)

Just as the Nazis appealed to the Jew’s rationality of self-preservation to induce cooperation, today, the West accepts an intensely surveillant regime as necessary for efficiency, convenience, productivity, national security, and national welfare and has abandoned critically thinking about the legitimacy of limitless surveillance technologies in private life. According to Bauman, when *efficiency, cost, convenience,* and *fear* displace personal integrity as the supreme authority and justification for political aims modern rationality has reached its potential.[[123]](#footnote-123) Whether surveillance technologies actually and empirically fulfill the functions they boast is not even considered, it is assumed. Surveillance is so rational a response to social needs, so normal, and so safe, complacency towards its appearance in private life has become a personal preference associated with sociability. The analytical paralysis renders Western society defenseless to the inherent totalitarianizing potential of these technologies.

A major oversight concerning the formalization of pervasive surveillance technologies is the presumption that the political context will remain relatively stable despite the inevitability that “at least some liberal democratic societies will devolve into forms of authoritarianism”.[[124]](#footnote-124) The danger lies in the fact that the institutionalized surveillance systems “will outlast contemporary political arrangements” and will be “just a fraction of the technological and informational inheritance awaiting any group that gains power”.[[125]](#footnote-125) As discussed above, the genocidal version of anti-Semitism only required a few key ingredients: a motive, the means, and the complete failure of modern liberal institutions. A simple analysis of new surveillance technologies demonstrates that just as modernity provided Hitler with the genocidal means, late modernity continues to support the genocidal political tradition. New surveillance technologies supply the means for an even more intrusive, and perhaps even more effective, invasion into private life where people could be identified, categorized, scrutinized, targeted, and marginalized at will with unprecedented precision. Late modernity also continues to fail to address the erosion of liberal democratic values. The only missing ingredient to a new age Holocaust is the motive.

**6. An Imperative for the Law and Lawyers.**

Bauman eloquently captures the totalitarianizing tendency of modern rationality stating, “the modern drive to a fully designated, fully controlled world…clash[es] with the pluralism of the human world”.[[126]](#footnote-126) It is the pluralism accorded by liberal institutions that must be diligently protected and fostered if the West seeks to avoid the totalitarianizing tendency of modern technology. In the tradition of Western liberal democracy, the Law must *always* and *only* be subversive to power. Regardless of privacy, security, cost and efficiency tensions, the Law must only interfere in private life if the minimum threshold of harm is met and must never subordinate procedures and proof. Liberal advocacy, the basis of a democratic legal system, cannot be restricted or influenced by a social desire to control drugs, prevent terrorism, or to secure the state.[[127]](#footnote-127)

According to Rainer Bucher, in the aftermath of the Holocaust Western societies must opt for individual rights and freedoms above any communal vision, must opt to identify with others rather than with political formations, and must orient the politic towards everyday life rather than the people within it (Bucher: 119). As the gatekeepers of the law, lawyers are morally obliged to vigilantly protect liberal advocacy, the sanctity and primacy of the person, legal equality, civil liberties, and procedural traditions. To protect privacy and autonomy from totalitarianizing surveillance technologies, the legal community must focus on the justification for surveillance in terms of pressing social needs, measurable outcomes, and whether the means and objectives of these technologies are rationally connected.[[128]](#footnote-128) Above all, the primacy of the advocate, civil rights and advocacy must always dominate legal ideology, education and legislation, and never judicial activism, the law and objectivity.[[129]](#footnote-129) Liberal institutions are the most precious safeguard against totalitarian tactics and politics because they protect a structure for society that ensures social pluralism and fluidity. In an era where modern technologies provide a limitless potential for totalitarianism, Western societies must remain unabashedly devoted to uphold the liberal and democratic principles of these institutions.

Legislation

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Privacy Act, RSC 1985, c P-21.

Secondary Materials: Articles

Abu-Laban, Yasmeen, “The Politics of Surveillance: Civil Liberties, Human Rights and

Ethics” in Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 420.

Adey, Peter, “Borders, Identification and Surveillance: New Regimes of Border Control”

in Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 193.

Andrejevic, Mark, “Ubiquitous Surveillance” in Kirstie Ball, Kevin Haggerty & David

Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 91.

Bauman, Zygmunt, *Modernity and the Holocaust* (Ithaca, NY: Cornell University Press,

1989).

Black, Edwin, *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany*

*and America’s Most Powerful Corporation* (Washington DC: Dialog Press, 2009).

Bruno, Fernanda, “Surveillance and Participation on Web 2.0” in Kirstie Ball, Kevin

Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 343.

Bucher, Rainer, *Hitler’s Theology: A Study in Political Religion* (New York: Continuum

International Publishing Group, 2011).

Ceyhan, Ayse, “Surveillance as Biopower” in Kirstie Ball, Kevin Haggerty & David

Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 38.

Cockfield, Arthur J, “Who Watches the Watchers? A Law and Technology Perspective

on Government and Private Sector Surveillance” (2003) 29 Queen's LJ 364.

DeCoste, FC, *On Coming To Law: An Introduction to Law in Liberal Societies*, 2nd ed

(Markham, ON: LexisNexis Canada Inc, 2007).

Fussey, Pete, & Jon Coaffee, “Urban Spaces of Surveillance” in Kirstie Ball, Kevin

Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 201.

Gandy, Oscar H, “Statistical Surveillance: Remote Sensing in the Digital Age” in Kirstie

Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 125.

Gellately, Robert, “The Gestapo and German Society: Political Denunciation in the

Gestapo Case Files” (1988) 60:4 *The Journal of Modern History* 654.

Haggerty, KD, “Visible War: Surveillance, Speed, and Information War,” in KD

Haggerty & RV Ericson, eds, *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2006) 250.

Haggerty, Kevin D, “‘Ten Thousand Times Larger...’: Anticipating the Expansion of

Surveillance” in Daniel Neyland & Benjamin J Goold, eds, *New Directions in Surveillance and Privacy* (London: Willan Publishing, 2009) 159.

Haggerty, Kevin D, “Surveillance, Crime and the Police” in Kirstie Ball, Kevin Haggerty

& David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 235.

Jenkins Jr, HW, “Google and the Search for the Future,” *Wall Street Journal* (14 August

2010) online:

<http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html>.

Jenkins, Richard, “Identity, Surveillance and Modernity” in Kirstie Ball, Kevin Haggerty

& David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 159.

Kerr, Ian & Jennifer Barrigar, “Privacy, Identity and Anonymity” in Kirstie Ball, Kevin

Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 386.

Koonz, Claudia, *The Nazi Conscience* (Cambridge, Massachusetts: The Belknap Press of

Harvard University Press, 2003).

Kren, George M & Leon Rappoport, *The Holocaust and the Crisis of Human Behavior*

(New York: Holmes & Meier Publishers Inc, 1980).

Kroener, Inga & Daniel Neyland, “New Technologies, Security and Surveillance” in

Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 141.

McGrath, John, “Performing Surveillance” in Kirstie Ball, Kevin Haggerty & David

Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 83.

Monahan, Torin, “Surveillance and Terrorism” in Kirstie Ball, Kevin Haggerty & David

Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 285.

Ploeg, Irma van der, “The Body as Data in the Age of Information” in Kirstie Ball, Kevin

Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 176.

Pridmore, Jason, “Consumer Surveillance: Context, Perspectives and Concerns in the

Personal Information Economy” in Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 321.

Raab, Charles D, “Regulating Surveillance: The Importance of Principles” in Kirstie Ball,

Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 377.

Reifner, Udo, “The Bar in the Third Reich: Anti-Semitism and the Decline of Liberal

Advocacy” (1986) 32 McGill LJ 96.

Rigg, Bryan Mark, 2nd ed, “Nuremburg Laws” (2012), online: The Jewish Virtual

Library: A Division of the American-Israeli Cooperative Enterprise <http://www.jewishvirtuallibrary.org/jsource/judaica/ejud\_0002\_0015\_0\_14977.html>.

Rule, James B, “‘Needs’ for Surveillance and the Movement to Protect Privacy” in

Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 64.

Steeves, Valerie, “Hide and Seek: Surveillance of Young People on the Internet” in

Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 352.

Turow, Joseph, and Nora Draper, “Advertising’s New Surveillance Ecosystem” in Kirstie

Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 133.

Webster, William R, “Public Administration as Surveillance” in Kirstie Ball, Kevin

Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 313.

Weikart, Richard, *Hitler’s Ethic: The Nazi Pursuit of Evolutionary Progress* (New York,

NY: Palgrave MacMillan, 2009).

Weller, Toni, “The Information State: A Historical Perspective on Surveillance” in

Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 57.

Wilson, Dean, “Military Surveillance” in Kirstie Ball, Kevin Haggerty & David Lyon,

eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 269.

1. Bauman, Zygmunt, *Modernity and the Holocaust* (Ithaca, NY: Cornell University Press, 1989) at 20. [↑](#footnote-ref-1)
2. *Ibid* at 13. [↑](#footnote-ref-2)
3. *Ibid* at 94. [↑](#footnote-ref-3)
4. Kren, George M & Leon Rappoport, *The Holocaust and the Crisis of Human Behavior* (New York: Holmes & Meier Publishers Inc, 1980) at 126. [↑](#footnote-ref-4)
5. Bauman, *supra* note 1 at 87. [↑](#footnote-ref-5)
6. Koonz, Claudia, *The Nazi Conscience* (Cambridge, Massachusetts: The Belknap Press of Harvard University Press, 2003) at 9. [↑](#footnote-ref-6)
7. Black, Edwin, *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America’s Most Powerful Corporation* (Washington DC: Dialog Press, 2009) at 54. [↑](#footnote-ref-7)
8. Bauman, *supra* note 1 at 32, 39. [↑](#footnote-ref-8)
9. Koonz, *supra* note 6 at 9, 42. [↑](#footnote-ref-9)
10. Weller, Toni, “The Information State: A Historical Perspective on Surveillance” in Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (London: Routledge, *forthcoming*) 57 at 58; Wilson, Dean, “Military Surveillance” in Ball, Haggerty & Lyon, *supra* note 10, 269 at 271. [↑](#footnote-ref-10)
11. Weller*,* *ibid* at 60. [↑](#footnote-ref-11)
12. Koonz, *supra* note 6 at 9. [↑](#footnote-ref-12)
13. Weller, *supra* note 10 at 61. [↑](#footnote-ref-13)
14. Bauman, *supra* note 1 at 73, 77. [↑](#footnote-ref-14)
15. Black, *supra* note 7 at 8. [↑](#footnote-ref-15)
16. Bauman, *supra* note 1 at 15. [↑](#footnote-ref-16)
17. Black, *supra* note 7 at 10. [↑](#footnote-ref-17)
18. *Ibid* at 56. [↑](#footnote-ref-18)
19. *Ibid* at 58. [↑](#footnote-ref-19)
20. *Ibid* at 169. [↑](#footnote-ref-20)
21. *Ibid* at 168. [↑](#footnote-ref-21)
22. *Ibid* at 9-10. [↑](#footnote-ref-22)
23. *Ibid* at 58. [↑](#footnote-ref-23)
24. *Ibid* at 50. [↑](#footnote-ref-24)
25. *Ibid* at 21. [↑](#footnote-ref-25)
26. Gellately, Robert, “The Gestapo and German Society: Political Denunciation in the Gestapo Case Files” (1988) 60:4 *The Journal of Modern History* 654 at 659. [↑](#footnote-ref-26)
27. *Ibid* at 677. [↑](#footnote-ref-27)
28. *Ibid* at 676. [↑](#footnote-ref-28)
29. *Ibid* at 665. [↑](#footnote-ref-29)
30. *Ibid*. [↑](#footnote-ref-30)
31. *Ibid* at 667. [↑](#footnote-ref-31)
32. *Ibid* at 668. [↑](#footnote-ref-32)
33. *Ibid* at 662, 668-91. [↑](#footnote-ref-33)
34. *Ibid* at 688, 690, 693. [↑](#footnote-ref-34)
35. Bauman, *supra* note 1 at 142. [↑](#footnote-ref-35)
36. *Ibid* at 130. [↑](#footnote-ref-36)
37. *Ibid* at 131. [↑](#footnote-ref-37)
38. *Ibid* at 118. [↑](#footnote-ref-38)
39. See Weikart, Richard, *Hitler’s Ethic: The Nazi Pursuit of Evolutionary Progress* (New York, NY: Palgrave MacMillan, 2009). [↑](#footnote-ref-39)
40. See Koonz, *supra* note 6. [↑](#footnote-ref-40)
41. DeCoste, FC, *On Coming To Law: An Introduction to Law in Liberal Societies*, 2nd ed (Markham, ON: LexisNexis Canada Inc, 2007) at 80. [↑](#footnote-ref-41)
42. *Ibid* at 202. [↑](#footnote-ref-42)
43. *Ibid* at 198. [↑](#footnote-ref-43)
44. *Ibid* at 215. [↑](#footnote-ref-44)
45. *Ibid* at 177. [↑](#footnote-ref-45)
46. Koonz, *supra* note 6, at 44, 46. [↑](#footnote-ref-46)
47. *Ibid* at 93. [↑](#footnote-ref-47)
48. *Ibid* at 96. [↑](#footnote-ref-48)
49. *Ibid* at 93-4. [↑](#footnote-ref-49)
50. *Ibid* at 96. [↑](#footnote-ref-50)
51. Rigg, Bryan Mark, 2nd ed, “Nuremburg Laws” (2012), online: The Jewish Virtual Library: A Division of the American-Israeli Cooperative Enterprise <http://www.jewishvirtuallibrary.org/jsource/judaica/ejud\_0002\_0015\_0\_14977.html>. [↑](#footnote-ref-51)
52. *Ibid*. [↑](#footnote-ref-52)
53. *Ibid*. [↑](#footnote-ref-53)
54. *Ibid*. [↑](#footnote-ref-54)
55. Reifner, Udo, “The Bar in the Third Reich: Anti-Semitism and the Decline of Liberal Advocacy” (1986) 32 McGill LJ 96 at 123. [↑](#footnote-ref-55)
56. Jenkins, Richard, “Identity, Surveillance and Modernity” in Ball, Haggerty & Lyon, *supra* note 10, 159 at 165. [↑](#footnote-ref-56)
57. Kerr, Ian & Jennifer Barrigar, “Privacy, Identity and Anonymity” in Ball, Haggerty & Lyon, *supra* note 10, 386 at 387. [↑](#footnote-ref-57)
58. Kroener, Inga & Daniel Neyland, “New Technologies, Security and Surveillance” in Ball, Haggerty & Lyon, *supra* note 10, 141 at 142. [↑](#footnote-ref-58)
59. Andrejevic, Mark, “Ubiquitous Surveillance” in Ball, Haggerty & Lyon, *supra* note 10, 91 at 92. [↑](#footnote-ref-59)
60. Fussey, Pete, & Jon Coaffee, “Urban Spaces of Surveillance” in Ball, Haggerty & Lyon, *supra* note 10, 201 at 205. [↑](#footnote-ref-60)
61. Andrejevic, *supra* note 59. [↑](#footnote-ref-61)
62. Ploeg, Irma van der, “The Body as Data in the Age of Information” in Ball, Haggerty & Lyon, *supra* note 10, 176 at 179; Adey, Peter, “Borders, Identification and Surveillance: New Regimes of Border Control” in Ball, Haggerty & Lyon, *supra* note 10, 193 at 195. [↑](#footnote-ref-62)
63. Webster, William R, “Public Administration as Surveillance” in Ball, Haggerty & Lyon, *supra* note 10, 313 at 313. [↑](#footnote-ref-63)
64. Adey*, supra* note 62; Ceyhan, Ayse, “Surveillance as Biopower” in Ball, Haggerty & Lyon, *supra* note 10, 38 at 38-9. [↑](#footnote-ref-64)
65. Andrejevic, *supra* note 59 at 92. [↑](#footnote-ref-65)
66. Weller, Toni, “The Information State: A Historical Perspective on Surveillance” in Ball, Haggerty & Lyon, *supra* note 10, 57 at 59; Haggerty, Kevin D, “Surveillance, Crime and the Police” in Ball, Haggerty & Lyon, *supra* note 10, 235 at 237. [↑](#footnote-ref-66)
67. Rule, James B, “‘Needs’ for Surveillance and the Movement to Protect Privacy” in Ball, Haggerty & Lyon, *supra* note 10, 64 at 69. [↑](#footnote-ref-67)
68. Kerr & Barrigar, *supra* note 57 at 389. [↑](#footnote-ref-68)
69. Abu-Laban, Yasmeen, “The Politics of Surveillance: Civil Liberties, Human Rights and Ethics” in Ball, Haggerty & Lyon, *supra* note 10, 420 at 421. [↑](#footnote-ref-69)
70. Monahan, Torin, “Surveillance and Terrorism” in Ball, Haggerty & Lyon, *supra* note 10, 285 at 287. [↑](#footnote-ref-70)
71. *Ibid* at 288. [↑](#footnote-ref-71)
72. Wilson, *supra* note 10 at 272. [↑](#footnote-ref-72)
73. Wilson, *supra* note 10 at 273; Haggerty, KD, “Visible War: Surveillance, Speed, and Information War,” in KD Haggerty & RV Ericson, eds, *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2006) 250 at 254-55 [Haggerty, “Visible War”]. [↑](#footnote-ref-73)
74. Haggerty, “Visible War”, *ibid* at 255. [↑](#footnote-ref-74)
75. Jenkins Jr, HW, “Google and the Search for the Future,” *Wall Street Journal* (14 August 2010) online: <http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html>. [↑](#footnote-ref-75)
76. Pridmore, Jason, “Consumer Surveillance: Context, Perspectives and Concerns in the Personal Information Economy” in Ball, Haggerty & Lyon, *supra* note 10, 321 at 323. [↑](#footnote-ref-76)
77. *Ibid*. [↑](#footnote-ref-77)
78. Kerr & Barrigar, *supra* note 57 at 387. [↑](#footnote-ref-78)
79. Kerr & Barrigar, *ibid* at 388. [↑](#footnote-ref-79)
80. Ceyhan, *supra* note 64 at 44. [↑](#footnote-ref-80)
81. Andrejevic, *supra* note 59 at 95. [↑](#footnote-ref-81)
82. Weller, *supra* note 10 at 62. [↑](#footnote-ref-82)
83. Turow, Joseph, and Nora Draper, “Advertising’s New Surveillance Ecosystem” in Ball, Haggerty & Lyon, *supra* note 10, 133 at 137. [↑](#footnote-ref-83)
84. *Ibid*. [↑](#footnote-ref-84)
85. *Ibid*. [↑](#footnote-ref-85)
86. *Ibid* at 138. [↑](#footnote-ref-86)
87. Webster, supra note 63 at 318. [↑](#footnote-ref-87)
88. Bruno, Fernanda, “Surveillance and Participation on Web 2.0” in Ball, Haggerty & Lyon, *supra* note 10, 343 at 343. [↑](#footnote-ref-88)
89. McGrath, John, “Performing Surveillance” in Ball, Haggerty & Lyon, *supra* note 10, 83 at 89. [↑](#footnote-ref-89)
90. Online: FYI Screening <http://fyiscreening.com/>. [↑](#footnote-ref-90)
91. Online: Employee Screen <http://www.employeescreen.com/>. [↑](#footnote-ref-91)
92. Online: Catchacheat <http://www.catchacheat.com/>. [↑](#footnote-ref-92)
93. Online: Abika <http://www.abika.com/>. [↑](#footnote-ref-93)
94. Online: Family Watch Dog <http://www.familywatchdog.us/ShowMap.asp>. [↑](#footnote-ref-94)
95. Online: Cop Watch <http://www.copwatch.org/>. [↑](#footnote-ref-95)
96. Online: Busted Mugshots <http://www.bustedmugshots.com/>. [↑](#footnote-ref-96)
97. Online: Blue Servo <http://www.blueservo.net/vcw.php>; also see Bruno, *supra* note 88 at 346-7. [↑](#footnote-ref-97)
98. Steeves, Valerie, “Hide and Seek: Surveillance of Young People on the Internet” in Ball, Haggerty & Lyon, *supra* note 10, 352 at 356. [↑](#footnote-ref-98)
99. Online: Wikileaks <http://wikileaks.org/>. [↑](#footnote-ref-99)
100. Andrejevic, *supra* note 59 at 94. [↑](#footnote-ref-100)
101. Abu-Laban, *supra* note 69 at 424. [↑](#footnote-ref-101)
102. *Ibid*. [↑](#footnote-ref-102)
103. Cockfield, Arthur J, “Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance” (2003) 29 Queen's LJ 364 at 366. [↑](#footnote-ref-103)
104. See “Guidance on Covert Video Surveillance in the Private Sector” (May 2009), online: The Office of the Privacy Commissioner <http://www.priv.gc.ca/index\_e.cfm>. [↑](#footnote-ref-104)
105. See “OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities” (March 2006), online: The Office of the Privacy Commissioner <http://www.priv.gc.ca/index\_e.cfm>. [↑](#footnote-ref-105)
106. SC 2000, c 5. [↑](#footnote-ref-106)
107. RSC 1985, c P-21. [↑](#footnote-ref-107)
108. Raab, Charles D, “Regulating Surveillance: The Importance of Principles” in Ball, Haggerty & Lyon, *supra* note 10, 377 at 383. [↑](#footnote-ref-108)
109. Kerr & Barrigar, *supra* note 57 at 392. [↑](#footnote-ref-109)
110. *Ibid*. [↑](#footnote-ref-110)
111. *Ibid* at 388, 392. [↑](#footnote-ref-111)
112. Cockfield, *supra* note 103 at 366-67. [↑](#footnote-ref-112)
113. *Ibid* at 367. [↑](#footnote-ref-113)
114. McGrath, *supra* note 89 at 83. [↑](#footnote-ref-114)
115. Haggerty, Kevin D, “‘Ten Thousand Times Larger...’: Anticipating the Expansion of Surveillance” in Daniel Neyland & Benjamin J Goold, eds, *New Directions in Surveillance and Privacy* (London: Willan Publishing, 2009) 159 at 160 [Haggerty, “Ten Thousand Times Larger”]. [↑](#footnote-ref-115)
116. Gandy, Oscar H, “Statistical Surveillance: Remote Sensing in the Digital Age” in Ball, Haggerty & Lyon, *supra* note 10, 125 at 127. [↑](#footnote-ref-116)
117. Haggerty, “Ten Thousand Times Larger”, *supra* note 115 at 173. [↑](#footnote-ref-117)
118. *Ibid*. [↑](#footnote-ref-118)
119. Bauman, *supra* note 1 at 85. [↑](#footnote-ref-119)
120. Haggerty, “Ten Thousand Times Larger”, *supra* note 115 at 162. [↑](#footnote-ref-120)
121. *Ibid* at 164-65. [↑](#footnote-ref-121)
122. *Ibid* at 162, 166. [↑](#footnote-ref-122)
123. Bauman, *supra* note 1 at 116. [↑](#footnote-ref-123)
124. Haggerty, “Ten Thousand Times Larger”, *supra* note 115 at 166-67. [↑](#footnote-ref-124)
125. *Ibid* at 166. [↑](#footnote-ref-125)
126. Bauman, *supra* note 1 at 93. [↑](#footnote-ref-126)
127. Reifner, *supra* note 55 at 123. [↑](#footnote-ref-127)
128. Raab, *supra* note 108 at 379-80. [↑](#footnote-ref-128)
129. *Ibid*. [↑](#footnote-ref-129)