[REVISED]

Privacy Fundamentalism:
An Essay on Social Responsibility

Alistair S. Duff

Introduction

Privacy faces an existential threat. Such assertions are of course unoriginal, not even controversial. State spying on entire citizenries, local council snooping, omnipresent cameras, targeted advertisements, employee monitoring, facial recognition, heat sensors, implanted devices, drones, smart uniforms, the internet of things, genetic profiling, neuro-imaging, artificial intelligence, and so on and so forth: there are so many actual or potential privacy harms that trying to list them is a fool's errand. Moreover, surveillance is now operating not only at the familiar level of sight, sound, and other observable senses; the "primary qualities" of space and time have also been compromised. The linear time and separate spaces which anchored privacy in the industrial era, have given way in the post-industrial age to a space-time continuum where privacy has lost all boundaries and all permanence. There remain, in Christena Nippert-Eng's vivid language, precious few "islands" of privacy (Nippert-Eng 2010).

It was all prophesied. Jeremy Bentham, a thinker "more important for the understanding of our society than Kant and Hegel" (Michel Foucault quoted in Vysniauskas 2018), foresaw the "inspection principle" governing not just prisons, but also mental asylums, schools, hospitals, factories, and welfare agencies (Bentham 1995 [1787]). Today each and every one of these social institutions has been allowed to fall under more or less complete electronic surveillance. It is not without significance that Bentham's original sketch for his "Panopticon penitentiary" has scrawled next to it a quotation from Psalm 139: "Thou are about my path, and about my bed: and spiest out all my ways..." (Bentham n.d.). Two hundred years later Theodore Roszak would denounce the quasi-religious "cult of information," a mindless worship of information technology and concomitant neglect of "the true art of thinking" (Roszak 1994). Now in the twenty-first century the situation is chronic. Personal privacy in the information society is profoundly "against the flow," at odds with the epoch's totems of transparency and connectivity. Of course, there are occasional interventions, "data protection" initiatives such as the recent European Data Protection Regulation, but with every step forward, it is not long before we find ourselves two steps back. No one can seriously doubt that, as a basic fact, privacy is in crisis.

It will be argued in this article that the only effective antidote to privacy's predicament is "privacy fundamentalism." This admittedly striking term has a documented history in privacy research. Introduced by the law professor and pioneering privacy researcher, Alan Westin, "privacy fundamentalists" are defined as persons "generally distrustful of organizations that ask for their personal information, worried about the accuracy of computerized information and additional uses made of it", and "in favor of new laws and regulatory actions to spell out privacy rights and provide enforceable remedies." They are different from "privacy pragmatists," who always "weigh the benefits to them of various consumer opportunities and services, protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved." Privacy fundamentalists differ even more from a third category of "privacy unconcerned," individuals who are "generally trustful of organizations collecting their personal information" and "ready to forego privacy claims to secure consumer-service benefits or public-order values" (Louis Harris Associates & Westin 1990; see also Kumaraguru & Cranor 2005).

Westin's surveys throughout the 1990s showed that approximately 25% of the United States public were privacy fundamentalists, compared with 55% pragmatists and 20% unconcerned. However, he detected a diminishing of the ranks of privacy fundamentalism after 9/11, in favour of pragmatism (Westin 2003). Westin's magnum opus, *Privacy and Freedom* (Westin 1967), while it inspired privacy advocacy around the world, was shot through with pragmatism. For example, after expounding numerous ethical shortcomings of "polygraphs," i.e. lie detectors, Westin ended by sanctioning their use, subject to certain conditions (Westin 1967, 263-267). A privacy fundamentalist would of course condemn these abominable and useless devices outright, as had Pope Pius XII (Westin 1967, 263). Not long before he died, Westin would defend even that egregious American privacy-eater, the Patriot Act (Fox 2013).

Today, in the face of all the new and impending threats, it is surely a philosophy of privacy fundamentalism, not pragmatism, that is needed. Pragmatism has been the de facto regnant philosophy for many decades, and it has signally failed to stem the tide of surveillance. A more robust position is needed, one that can fortify the dwindling band of citizens still prepared to make a principled stand for privacy. Little privacy loses the final argument with the big battalions of money and power: that is the underlying script that must be rewritten. Now some people might fully agree that privacy fundamentalism in Westin's sense is required, but think that it should go by another, less off-putting, name. It is likely, indeed, that Westin's use of it was all along an attempt to discredit the position it represents. However, the very shock-value of "fundamentalism" is at least helpful in calling attention to the extremely high stakes at issue. If the battle for privacy is to have any chance of being won, a dramatic vocabulary may prove to be an indispensable part of its arsenal. Anyway, labels aside, the rudiments of the content of a theory of privacy fundamentalism are ventured below.

Elements of Privacy Fundamentalism

The place to commence a defence of privacy is of course at the very beginning. It is obvious that privacy has been at a disadvantage literally from "day one." The Book of Genesis teaches that humanity's original, Edenic state was one in which privacy was totally absent. According to that super-seminal text, it was only after the "fall" that Adam and Eve tried to hide their "private parts." At the other end of the eschatological scale, the Book of Revelation draws a picture of a future heaven of choirs and communion; indeed, the very idea of desiring privacy seems antithetical to a perfected state, religiously understood. It is hardly surprising then that the word "private" occurs only once in the whole of John Milton's multivolume epic *Paradise Lost*, according to John Hollander (Hollander 2001, 22). The connotation of weakness, negativity, clings to privacy from start to finish. That much is evident in the cultural gene-pool of Christendom.

Secular history, too, has always made privacy subordinate to the public, the political. In evolutionary rationales, survival meant that the group had to take precedence over the individual. As civilization came on stream, Aristotle would define "man" as a political animal. It was in the polis, the public arena of democratic deliberation and decision-making, that a man was in his element, was free; the domestic sphere, the "oikos," was a subsidiary, necessitous, invisible realm, a back zone into which Aristotle notoriously consigned women, children, and slaves (Aristotle 1941 [c. 330 BC]). Privacy was indeed the realm of the "oik", the idiot. This negative valuation carried over into the Roman world. The very word "privacy" shares the same Latin root as terms like "privation" and "deprivation." It is no accident then that in Britain, its ruling class raised on Greek and Latin literature, elite schools are still called "public schools," or conversely that the lowest rank in the British army is that of "private." And this also perhaps explains why most of the outstanding contemporary privacy theorists are female, as will be seen.

The deep-seated anti-privacy prejudice was never properly addressed in western thought. “What is surprising,” writes Lucas Introna, “is that privacy did not get explicit attention from any of the great liberals. Locke, Rousseau, van Humboldt, and J. S. Mill did not spend as much as a page on the subject” (Introna 1997, 261); nor, it might be added, is the idea of privacy salient in the writings of John Rawls, the twentieth-century philosopher who arguably completes the liberal canon. To be sure, private property is a major theme of all of these eminent thinkers, but privacy rights have no necessary connection with any form of ownership. Neither does privacy get a mention in the United States Constitution, although it was subsequently supposedly spotted in the “penumbra” of that great constitution. It would seem then that most commentators are agreed that, under liberalism, privacy should “wear the character of exceptions” (Bentham quoted in Hixson 1987, 102).

However, whatever might have been appropriate or tolerable yesterday, in the information society we inhabit now privacy needs to come out of the shadows. Privacy cannot—in an age where information, including personal information, is flowing in all directions in ever-greater abundance—remain a secondary or derivative right, merely implicit in the first-order goods of liberty of speech, association, and the like. It needs to be a first-order political good in its own right, part of liberal-democracy’s exterior, not just its remote interior. This is the central thesis of privacy fundamentalism.

Before seeking to establish privacy’s value, however, a working definition is required. No trivial matter, this is actually very much a challenge for any theory of privacy. Westin famously construed privacy as “the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin 1967, 5), a way of understanding it that is clearly suited to the information age. Since he wrote, though, much philosophical energy has been spent on whether “determining” does actually belong in the definition. Anita Allen, herself noted for being the first philosophy professor to have written a monograph on privacy, maintains that there is such a condition as unwanted and unpopular privacy, and that access rather than control is therefore the relevant yardstick (e.g., Allen 2011). However, Beate Roessler, another leading contemporary privacy philosopher, claims that “the moment of conscious control does seem to be constitutive for the meaning of privacy” (Roessler 2005, 195). Ordinary language, Roessler reasons, treats privacy positively, with normative and not merely descriptive content; it would not be natural to say of someone stuck in a crevasse that they had privacy (Roessler 2005, 7).

Allen’s position on this is more convincing. Privacy is indeed often enforced, as revealed by frequent controversies over the compulsory veiling of girls and women. The flaw in control definitions is that they always end up collapsing privacy into adjacent concepts such as liberty and autonomy. This has resulted in the invention by the United States Supreme Court of “decisional” privacy, cited with far-reaching effects in the decriminalization of abortion, and much subsequent legislation. Yet, whatever the rights and wrongs of abortion, it is straining language too far to refer to it as a matter of privacy. Abortion is at bottom a liberty issue—the mother’s liberty, if not the foetus’s. Privacy fundamentalism, like all fundamentalisms, will endeavour to keep things simple, defining privacy in as basic a way as possible, that is, as a neutral, descriptive concept; and from that firm basis proceed to identify what kinds of normative arguments can be marshaled.

So the following discussion will follow Allen in defining privacy in terms of unavailability or, to adopt David O’Brien’s more memorable formula, as “an existential condition of limited access” (O’Brien 1979, 16); and it will be confined to the privacy of individuals, not groups or institutions. The substantive task now is to establish that this condition denotes a fundamental human good. While space will not allow a detailed exposition, the coordinates of a case for privacy as a fundamental value can be provided.

First, the human need for privacy is what anthropologists call “a cultural universal.” Westin’s book serves again as a useful benchmark, since it summarizes scientific data from a range of reputable sources. For example, Westin referenced work on the fascinating Tuareg tribes of North Africa. While living communally in a way that cannot accommodate western expectations regarding privacy, Tuareg menfolk achieve similar ends by the simple expedient of veils, continuously adjusted according to company. Other societies make good use of masks or fans, Westin notes; Hollywood actresses, other defenses breached, resort of course to sun-glasses. “The Tuareg veil,” Westin soundly deduces, “is a symbolic realization of the need for privacy in every society” (Westin 1967, 13). Nowadays, it might be said that these are all examples of “privacy-enhancing technologies,” or ways of executing different “privacy settings.”

Japan is another instructive case study, as recent research demonstrates (e.g. Mizutani et al. 2004, Murata & Orito 2008; Nakada & Tamura 2005). The paper walls in traditional Japanese houses and the nudity norm in public bath-houses have occasioned the common perception of a nation lacking in consciousness of personal privacy rights. Its group-minded, family-centric culture high in social capital supposedly leaves no room for privacy. Indeed, the word does not even exist in the Japanese language, which must get by with the American loan word “puraibashii.” Ergo, the Japanese do not value individual privacy. However, this is a complete misreading of the situation. They do bathe naked, but they preserve gender boundaries punctiliously. The walls in their houses can be thin, yet a taboo on eavesdropping and indiscretion preserves the privacy peace. They do not have a direct equivalent for “privacy” but they have plenty of cognate terms, such as kodoku (solitude) and himitsu (secrecy). Like the Tuareg, then, the Japanese just “do” privacy differently.

All the evidence indicates that privacy is a cultural universal (see especially Moore 2018 and van der Geest 2018). In the terms of the present article, privacy is a “cultural fundamental,” and its being such is the scientific spine of the case for privacy fundamentalism. However, if privacy is to be properly founded, privacy fundamentalism needs to dig deeper. While privacy is undoubtedly a cultural fundamental, its precise content is by all accounts geographically variable. It also changes over time. Indeed, “time-honoured” legal barometers such as “reasonable expectation of privacy” are under immense pressure, now that it is beginning to feel unrealistic to expect any privacy, especially outside the home, at least in the West. Arguments at the empirical level can thus only take us so far.

It is at this point then that the theory of privacy needs to risk becoming more contentious. Privacy fundamentalism postulates that privacy cannot be secured unless some kind of metaphysical case is made for it, in addition to all the empirical data. Specifically, it is the proposal of privacy fundamentalism as understood here that privacy’s value must be anchored in an unchanging reality, an objective spiritual and moral order existing independently of the empirical world. Of course, this is not a fashionable kind of claim. Graham Sewell and James Barker are probably expressing western scholarly opinion much more faithfully when they present privacy as a principle that sternly rejects “eschatology” and “universal ontological categories” (Sewell & Barker 2001, 187). However, majority academic opinion is not necessarily either morally right or socially expedient.

According to privacy fundamentalism, privacy is an essential condition for the flourishing of the inner self, that is, of the “soul;” and its being so makes personal privacy inviolable. At one level, this is hardly an esoteric claim: our basic instincts scream that privacy is infinitely precious, as well as inscrutable. The tricky philosophical issue is how to ground these familiar intuitions. Of course, it would not do to try to fasten them onto the axioms of religious fundamentalism, eschatological or otherwise, since while most ordinary people are in some sense religious, they are mostly not fundamentalists. Hence a broader metaphysical argument is called for. Here idealism, and specifically British idealism, a nineteenth-century school of thought currently undergoing intensive reappraisal (e.g., Boucher & Vincent 2012; Duff 2015; Mander & Panagakou 2016; Tyler 2017), can, it is suggested, supply extremely helpful pointers. Although the idealists did not focus on privacy per se, their general worldview, developed in response to the naturalism of their own day, contained powerful concepts that can be repurposed for the promotion of one of the greatest causes of the twenty-first century.

Their central claim was that there is an "ideal" world as well as a natural one. "The real man," T. H. Green, the founder of British idealism, asserted, "is not an object of observation" (Green 1886a, 108). Our very consciousness, he continued, implies the existence of a further, invisible, reality. It is necessary, therefore, to make an essential distinction between our "empirical" selves, belonging to the sensible world and hence accessible to psychology and anthropology, and our "real" selves, which exist somehow outside of space and time (Green 2003, 189). This ideal order is unverifiable, to be sure, and the right of privacy can never therefore be positively demonstrated. However, as Green astutely pointed out, *all* rights and values are insensible and therefore both unverifiable and, by the same token, unfalsifiable (Green 1886b, 362). That does not necessarily make them unreal; quite the opposite. The case for privacy, as indeed for liberty and other more widely acknowledged ethico-political values, can be rendered in terms of its being necessary for the flourishing of this real self.

Green and many other idealists went a step further and invoked a divine consciousness, of which human consciousness, they deduced, formed a part, and to which reason and conscience served as a conduit. The real self is part of this hallowed world, and so privacy, it can be inferred, protects what is sacred. To reiterate, this is not religious fundamentalism, although it is compatible with such; it is an inclusive way of establishing privacy not just as a *cultural* fundamental but also as some kind of *spiritual* fundamental. Its salutary effect, if accepted, is a reversal of the worldly, Aristotelian identification of the real self with the public realm. Man, on this alternative view, is not essentially a political animal, but rather a spiritual being—and to realise that essence, she needs privacy. While the outer self is empirical, part of the physical word, the real self is spiritual, metaphysical, ideal. This is not to say that we have two selves. It is rather that the real, inward self is ontologically prior to the staged self, the self-for-others. The real self is what needs affirmation, because it is this that is the ultimate target of totalitarianism. In such a light, it is legitimate, and given current dangers surely politically desirable, to call the right to privacy sacred.

In saying that privacy is necessary for the protection of the real self, it might seem that privacy is thereby being demoted from a fundamental to an intermediate or instrumental good. In one sense, the point must be conceded. Privacy is not an ultimate, still less *the* ultimate, good. It logically cannot be, because privacy is a relation, and therefore not the kind of category that can be the possessor of ultimate value. However, as Roessler has clearly explained, foregrounding privacy does not mean that one cannot also ground it in a further value (Roessler 2005). In her case, that ultimate value is a modernistic notion of individual autonomy. In our case, it is a traditional notion of the spiritual welfare of the soul. The key claim for present purposes is that privacy can and should be treated as a first-order political good. It is again exactly the same in this respect as liberty. Liberty is no more a final good than is privacy; liberty is also a relation, also therefore necessarily intermediate. Yet liberty is by all accounts endorsed as a first-order political good. Privacy fundamentalism only requests the same consideration for privacy.

Privacy Fundamentalism in Context

Privacy is thus a fundamental good, in the sense of being both empirically universal and spirtually essential, but as has been suggested above it is also to some extent culturally, and more generally, contextually, sensitive. Again, this should not be too puzzling, since the same is true of other first-order political goods. A primitive privacy fundamentalism might try to insist that privacy is an "absolute" that always trumps every other claim, but a sophisticated and viable privacy fundamentalism must accept that privacy is not the only important value. Privacy claims are not necessarily valid, because they can be outweighed by other values, such as freedom—of information or of the press, say—not to mention national security. The truth is that nothing is inalienably either private or public. For example, no item, in ordinary circumstances, could be more public than surnames, yet a surname must become terribly private the moment that it is in danger of winding up on a terrorist hit-list. It all depends on the context. So to have credibility, privacy fundamentalism needs to be compatible not only with the overall technological and political environment, but also with the specific social worlds within which innumerable information disclosures have to take place.

The most important contemporary case for a contextual approach is that of Helen Nissenbaum, herself also a strong advocate of privacy rights, if not necessarily a privacy fundamentalist in the sense under development here. In her remarkable and widely influential treatise *Privacy in Context*, Nissenbaum disputes the common attachment of privacy to special places, such as the home, and to special information, such as intimate personal details. Such equations, based on a rigid dichotomy of private versus public, do not account for some of our basic intuitions about privacy, she argues. For example, they do not allow for privacy in public or in the workplace; they also position privacy too close to secrecy, an association that has done privacy's reputation much damage (Roessler 2010, 103-126).

In place of these brittle, unsustainable distinctions, Nissenbaum offers a theory of privacy as "neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information" (Nissenbaum 2010, 127, italics in original). Appropriateness depends on the situation. Echoing Ferdinand Schoeman's observation that "one important function of privacy is to help maintain the integrity of different spheres of life" (Schoeman 1992, 157), Nissenbaum crafts an innovative benchmark that she calls "the framework of contextual integrity." (Roessler 2010, 127-157) This framework specifies the mix of values, purposes and practices that make a particular social domain, for example medicine or banking, what it is. Thus, the purpose of medicine is the health of patients, and all conduct in a medical context should reflect norms associated with that purpose, informational norms included. It is consonant with medicine that patients should reveal their health data, including details whose disclosure would be highly inappropriate in any other context. Yet if a health professional were to ask for a patient's bank statements, that would constitute a privacy infringement, financial data being entirely irrelevant to the medical context. The situation is exactly reversed in the social context of interactions with one's bank manager.

The upshot is that information should only be transmitted in a way appropriate to the situation at hand. Privacy fundamentalism, despite its stringent ethic and its anchorage in a putative ideal reality, concurs that no information is so secret that its transmission can never be justified. It maintains, nevertheless, that violations of contextual integrity have become a rampant evil which must now be stopped.

A disputatious stance is integral to privacy fundamentalism. However, establishing privacy as an essential value, and a moral right to which persons in every tribe and nation are entitled, does not mean that this right should always be reified in law. That too depends entirely on the circumstances. The cardinal political error of religious fundamentalism, as in both Christian Puritanism and Islamic Shariah Law, is its failure to grasp the difference between sin and crime. People have rights to love, respect and many other good things, but it is not always appropriate to enforce such claims; and privacy is no different. Even lawyers Samuel Warren and Louis Brandeis' seminal article "The Right to Privacy" (Warren & Brandeis 1890), while setting out for the first time the case for a presumptive general right to privacy, pled only for citizen redress against one specific intrusion, namely, press photographing of private dwellings. More recently, Priscilla Regan has demonstrated that "legislating privacy" only works effectively in the modern world when general principles are "reducible to clear legal rules" (Regan 1995, 178). Privacy fundamentalism does not, therefore, aim for an all-purpose, almighty Privacy Torah. Nevertheless, privacy fundamentalism will be prepared to wield the civil sword when necessary. In situations where personal privacy is in manifest danger, state action is sometimes, as a last resort, the correct mode of protection.

Policy Applications of Privacy Fundamentalism

Now that the nuts and bolts of a theory of privacy both fundamentalist and flexible are in place, it is possible to proceed to apply it to concrete issues. The following will be considered: closed circuit television, encryption, and newspaper exposés. This is admittedly only a small sample of issues, but it is one that addresses notoriously hard cases, and that traverses a wide social and political terrain. While the treatment can only be introductory, it will seek to indicate in outline that privacy fundamentalism is not about stemming necessary flows of information in the information society, but about securing an "existential condition of limited access" in modern, morally complex socio-technical situations.

"Despite consistent poll results showing concern about something called 'privacy'," John Gilliom writes, "technologies which would have once looked Orwellian now mark the face of the social landscape" (Gilliom 2001, 124). The expansion of "cctv" is well advanced in the United Kingdom, the United States, and many other countries. Cameras have been placed, by authorities of various kinds, in streets, classrooms, courtrooms, parks, airports, swimming pools, music venues and innumerable other locations. The public remains largely oblivious. For a start, most of the cameras are not actually "closed circuit;" they are open circuit, that is, linked to the internet. According to the Royal Academy of Engineers, "the continued use of the term [cctv] is an indicator of a general lack of awareness on the nature of contemporary surveillance" (Royal Academy of Engineers 2007, 33). The UK's official watchdog now recommends they be referred to as "video surveillance camera systems" (Surveillance Camera Commissioner 2018, 12). However, whatever they are technically, they are a massive problem normatively. Omnipresent cameras clash with precisely the human essence that privacy should protect. They make us act as though we are on parade; we become targets, suspects, objects. For Roessler, such surveillance forces a shift from a first-person to a third-person perspective, resulting in "a loss of autonomy in terms of the authenticity of one's behaviour, which is turned into behaviour *as if*, that is alienated behaviour" (Roessler 2005, 129). Idealistically-speaking, it oppresses the real self, the soul.

Admittedly, official video surveillance has not yet invaded the home, unlike the infamous "telescreens" in *Nineteen Eighty-Four* (Orwell 1949). Yet, as Nissenbaum has emphasised, people should have some privacy even in public (Nissenbaum 2010). Where the world beyond one's front door becomes immediately a panopticon, the social fabric has basically unraveled. The integrity of the ordinary activity—sipping coffee in the plaza, dancing at a rock concert, the quiet woodland stroll—has been fatally compromised; the time-honoured verities of presumption of innocence, reasonable suspicion, and due process have disappeared. Privacy fundamentalism must therefore problematize the relentless roll-out of video surveillance and its attendant technologies. The increasing addition of microphones and loudspeakers to video surveillance cameras in the UK—"Pick up that litter you just dropped!" (Clout 2007)—is a blatantly Orwellian innovation. An ongoing campaign by Britain's best privacy pressure group, Big Brother Watch, is thus worthy of a citation. Called "Face Off", it confronts the British police's disproportionate use of automatic facial recognition cameras, deployed at Champions League matches, Stereophonics gigs, Notting Hill carnivals, and even Remembrance Sunday services (Big Brother Watch 2018).

None of this need entail universal proscription. In Germany, a more or less complete ban on street cameras is in place, and this is totally understandable in light of that country's specific history of state takeover by a genocidal totalitarian party. However, for other western democracies a less draconian stance may be appropriate. Indeed, the very nature of some public spaces makes supervision morally uncontroversial. Car parks, for example, do not lose their contextual integrity if they are under round-the-clock surveillance, since their function is strictly limited to safe harbor of expensive metal objects. The environs of pubs and clubs with track records of violence are also a fitting location for cameras; indeed, where the problem is known to be acute, cameras *inside* these venues might be legitimate, since conducive to their intrinsic end of people's enjoyment. But most cultural and political activities should not be officially monitored; and only the most crime-prone urban and rural spaces should be permanently wired up. Of course, if a terrorist cell or a serial killer is known to be working a particular area, then blanket surveillance could be justified until they are caught, but such circumstances are exceptional. History confirms that the removal of personal privacy is the essence of authoritarianism; and the scale of video surveillance that liberal-democracies are now allowing can only lead to that frightful end.

That the defense of privacy is compatible with law and order comes through in my next example. It might be thought that encryption, the making of computer communications indecipherable, is a "slam dunk" for privacy fundamentalism. It was the issue that galvanized the privacy movement in the 1990s in its opposition to the "Clipper chip," the authorities' backdoor key to electronic messages (Gurak 1997). It is still a cause célèbre in Silicon Valley, bound up with cyber-libertarian philosophy and its genetic antipathy to state power. The right to perfect encryption is highly questionable, however. While official spying of the populace as a matter of course is indeed unacceptable, as incompatible with the fundamental political context of democracy, the investigation of genuine suspects is not. But if digitized messages cannot be read, then the police cannot do their jobs in the special context of criminal investigations. Instead, an anarchic zone "above the law" is created, and carte blanche given to organized crime and other evil-doing. This too is unacceptable. There is, to be sure, a "black box" that privacy fundamentalism must protect, but it contains the human soul, and that alone. Thus privacy fundamentalism on this issue converges with what feminists have long argued, that privacy should not be a shield for abuse (DeCew 2015). The 2015 massacre in San Bernadino, California, after which Apple, citing privacy concerns, refused to help the Federal Bureau of Investigation to access an iPhone belonging to one of the terrorists, illustrates as clearly as anything could the difference between a true and a false privacy fundamentalism. All Tim Cook, Apple CEO, really achieved by his stubborn stance was to bring privacy into disrepute (Duff 2016; see also Bay 2017). The American Library Association, it should be noted, begs to differ (American Library Association 2016).

Privacy fundamentalism will never hinder the authorities in the legitimate conduct of their business. However, finally, privacy fundamentalism will also often support the state's perennial adversary, a free and investigative press. Press freedom is of course one of the best established first-order democratic values, and privacy is usually cast as being in conflict with it. But on closer inspection, the antithesis is revealed to be only superficial. An essential function of the press is to act as a "watchdog" on all forms of social power, and where the common good necessitates penetration into private spaces, its interventions can be legitimate. Indeed, even the sharpest forms of press intrusion, such as undercover operations, are sometimes justifiable. Now it might be thought that these are precisely the kinds of activities that a fundamentalist-Nissenbaumian approach would condemn: for what is such work if not a rude unraveling of the social fabric, eventuating in revelatory headlines like "Concealed Tapes Catch Sports Coach Plotting to Fix Games?"

However, privacy fundamentalism would actually tend to support the press in such cases. While the context of a supposedly private conversation in a "sting" is indeed compromised, the press thereby serves the intrinsic purposes of sport—sportsmanship, fair competition, gratification of the hero-worshiping public—far more faithfully than corrupt coaches. The latter's real selves are not trespassed upon in any meaningful sense, their “existential condition of limited access” hardly nullified. Privacy only ever demands an *appropriate* restriction of personal information, and in a great many media exposés the supervening context of a bona fide inquiry palpably in the public interest implies that the transmission of embarrassing or incriminating personal information is ultimately justified. It is thus quite congruous that some of the staunchest supporters of the press and of freedom of expression and information, such as the American Civil Liberties Union and the Electronic Frontier Foundation, are also great champions of privacy. Indeed, an investigative press remains by far the strongest bulwark of the privacy of ordinary people. The moral of all these sketches—they do not claim to be anything more—is that privacy fundamentalism requires as much careful casuistry as privacy pragmatism and any other philosophy of privacy.

The Personal Practice of Privacy Fundamentalism

Such in outline is the theory of privacy fundamentalism. However, it would not be fundamentalism at all if it were only theory, because fundamentalism demands the outworking of principles in personal practice: it is never just an abstract theory but also a “philosophy of life.” Much of the ablest recent privacy apologetics has sought to compute privacy’s value to society (e.g., Lever 2011; Roessler & Mokrosinska 2015; Solove 2008; Waldman 2018). However, it is the individual who is finally at the center of privacy fundamentalism, the individual poised—at least sometimes—against society. Now the characteristic modes of fundamentalist praxis are obvious: counterculturalism, anti-establishmentarianism, protestology. Those who want to conserve privacy need to be prepared to act in such ways against the increasing onslaught of surveillance in all its guises. Instead, more and more citizens are morphing into privacy pragmatists or even privacy unconcerned, in Westin’s language, “knights of infinite resignation” in Soren Kierkegaard’s. Judgment cannot be too harsh: it is easy to fall into the temptation to believe that the “technological imperative” cannot be disobeyed, that the “surveillant assemblage” is too imbricated in our lives to be undone, and therefrom either to make too many concessions or to give up caring altogether. But that is not how a *fundamentalist* thinks; she or he is governed by faith and hope, not despair, and only by walking that narrow way, I am suggesting, will we be delivered from the evil of technocracy.

This does not mean that every encroachment by technology, every infringement of contextual integrity, can be resisted. Battles need to be picked carefully. However, we should all be prepared to be a little more awkward next time the local council or the dentist demands irrelevant information, next time a private company requires inordinate data input, next time our employer pilots a new form of digital tracking, and next time a camera appears in a facility that we frequent. We, the citizenry, need to say openly, “I think that that is an invasion of privacy,” and to take the trouble to write a letter or email to management, to the union, to the newspaper. This kind of individual action is largely missing today, but it is where—at the “grassroots”—resistance should be happening.

The forces of panopticism are overwhelmingly superior to whatever is available on the other side. Now, as with any unequal struggle, this sooner or later poses the agonizing question of the legitimacy of extra-parliamentary and illegal behavior. Privacy fundamentalism should not be seduced into the extremist ways of Luddism. Fearing for their livelihoods as craftsmen, the original Luddites smashed the machines of the early industrial revolution, threatening the property, privacy, and personal safety of individuals whom they associated with the new economic order. Today neo-Luddites, so-called, indulge in computer hacking and other forms of sabotage; on their fringes there is even support for the “unabomber,” Ted Kaczynski, who from his filthy forest hideout prosecuted a lethal letter-bomb campaign against those he counted members of the “scientific-technological establishment” (Jones 2006, 222-227). That is emphatically not the spirit of a privacy fundamentalism resting on idealism and deontological ethics, and engaged with the real world. Privacy fundamentalism does not involve a blanket denial of technological progress, it does not demonize the "information revolution," and it certainly does not condone any form of violence.

Nevertheless, one step that may reluctantly need to be taken is "obfuscation." That is to say, privacy fundamentalism points to the conclusion that incomplete or inaccurate personal data should in some cases be given where there are exorbitant requests for information—for example, a survey that impudently demands intimate lifestyle facts, or an airline that insists upon a mobile phone number. It is increasingly frequently the case that without filling in such data, it is impossible to proceed with an online booking or other service. In such cases, privacy fundamentalists will, arguably, sometimes need to enter false data. This is the conclusion at which Nissenbaum has arrived as well, no doubt equally reluctantly (Brunton & Nissenbaum 2015; see also Hauptman 2018).

It is possible that a strict Kantian would denounce obfuscation as a form of lying, but the riposte has to be that one is effectively left with no choice. Web 2.0 technologies do not allow one to plead a "fifth amendment;" one must either input data or one is discontinued; but if the request compromises one's privacy, and this is so in a multiplicity of contexts, and if there is no realistic alternative to using the service, then even a robust morality of duty surely cannot necessitate self-incrimination and the "selling of one's soul." Consciences can be cleared by the reflection that one is really "lying," if lying it is, to machines and systems, not to fellow human beings; and that obfuscation is being resorted to, not with a hand on a Bible in the witness box, but in an impersonal technological matrix for whose existence the subject has never been given the right of consent. If enough people subvert the system in this way, it will become unworkable, and a fundamental change in societal direction may become possible. At any rate, the individual will have protected her privacy and saved herself from being merely another captive of the cult of information.

Conclusion

We are becoming totally "informatized," with ubiquitous surveillance an inevitable and unwelcome corollary of this process. Surveillance's antithesis and antidote, personal privacy, has long been an aspect of liberalism's interior, an indispensable backdrop to the iconic democratic principles of liberty, justice, etc, yet it has somehow never graduated into a first-order value in its own right. This is the anomaly that has to be rectified. Now—in the age of information—privacy must assume its rightful place at the forefront of major political categories. An attempt has been made in the present article to offer some preliminary tenets of such a theory of privacy, what has been called, adopting a term introduced by privacy leader Alan Westin, "privacy fundamentalism." With privacy defined as an individual's existential condition of limited access, privacy fundamentalism plants the right to privacy not just in cultural universalism but also in a metaphysics of the self, of the "real" self, a position that has been extrapolated from the resurgent idealist worldview. I have tried to articulate a strong theory of privacy, but one that is also fully compatible with the complicated contexts of competing considerations in the real world. Details aside, however, the main message is stark. Privacy's cause will soon be lost completely if it continues to be fought merely pragmatically. Like the bodily sacrilege of torture, the violation of the spiritual state of privacy must be rejected without equivocation simply "because it is wrong" (Fried & Fried 2010).

References

Allen, A. L. (2011). *Unpopular privacy: What must we hide?* Oxford. Oxford University Press.

American Library Association (2016, February 26). Demand for Apple encryption tool threatens library users' privacy, press release. Chicago, IL: ALA. Available at http://www.ala.org/news/press-releases/2016/02/demand-apple-encryption-tool-threatens-library-users-privacy

Aristotle (1941 [c. 330 BC]). *Politics*. In *The basic works of Aristotle,* R. McKeon (Ed.). New York, NY: Random House.

Bay, M. (2017). The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. *First Monday*, 22(2). Available at: <https://firstmonday.org/ojs/index.php/fm/article/view/7006>

Bentham, J. (n.d.) *Bentham papers*. University College London Library Special Collections, box cxix, folio 47.

Bentham, J. (1995 [1787]). *The panopticon writings,* intro. M. Bozovic. London: Verso.

Big Brother Watch (2018). *Face off: The lawless growth of facial recognition in UK policing.* London: Big Brother Watch. Available at https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

Boucher, D., and A. Vincent (2012). *British idealism: A guide for the perplexed*. London: Continuum.

Brunton, F., and H. Nissenbaum (2015). *Obfuscation: A user's guide for privacy and protest.* Cambridge, MA: The MIT Press.

Clout, L. (2007, April 4). Talking CCTV gives Big Brother a voice. *The Daily Telegraph*. Available at https://www.telegraph.co.uk/news/uknews/1547550/Talking-CCTV-gives-Big-Brother-a-voice.html

DeCew, J. W. (2015). The feminist critique of privacy: Past arguments and new social understandings. In B. Roessler and D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 85-103). Cambridge: Cambridge University Press.

Duff, A. S. (2015). Cyber-Green: Idealism in the information age. *Journal of Information, Communication and Ethics in Society*, 13(2), 146-164.

Duff, A. S. (2016, March 26). Apple is wrong in its refusal to unlock phone. *The Scotsman*. Available at https://www.scotsman.com/news/opinion/alistair-s-duff-apple-wrong-in-its-refusal-to-unlock-phone-1-4083235https://www.scotsman.com/news/opinion/alistair-s-duff-apple-wrong-in-its-refusal-to-unlock-phone-1-4083235

Fox, M. (2013, February 22). Alan F. Westin, who transformed privacy debate before the web era, dies at 83, *The New York Times*. Available at https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html

Fried, C., and G. Fried (2010). *Because it is wrong: Torture, privacy and presidential power in the age of terror*. New York, NY: W. W. Norton.

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

Green, T. H. (1886a). Lectures on the philosophy of Kant. In *Works of Thomas Hill Green*, Vol. 2, R. L. Nettleship (Ed.) (pp. 2-154). London: Longmans, Green & co.

Green, T. H. (1886b). Lectures on the principles of political obligation. In *Works of Thomas Hill Green*, Vol. 2, R. L. Nettleship (Ed.) (pp. 335-553). London: Longmans, Green & co.

Green, T. H. (2003). Notes on moral philosophy. In *Miscellaneous Writings, Speeches and Letters*, P. Nicholson (Ed.) (pp. 188-192). Bristol: Thoemmes Press.

Gurak, L. J. (1997). *Persuasion and privacy in cyberspace: The online protests over Lotus MarketPlace and the Clipper Chip*. New Haven, CT: Yale University Press.

Hauptman, R. (2018). A mildly radical solution to privacy encroachments. *Journal of Information Ethics*, 27(2), 22-25.

Hixson, R. F. (1987). *Privacy in a public society: Human rights in conflict*. New York: Oxford University Press.

Hollander, J. (2001). The language of privacy. *Social Research*, 68(1), 5-22.

Introna, L. D. (1997). Privacy and the computer: Why we need privacy in the information society. *Metaphilosophy*, 28(3), 259-275.

Jones, S. E. (2006). *Against Technology: From the Luddites to Neo-Luddism*. New York, NY: Routledge.

Kumaraguru, P., and L. F. Cranor (2005). *Privacy indexes: A survey of Westin's studies*. Pittsburgh, PA: Institute for Software Research International, Carnegie Mellon University. Available at https://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf

Lever, A. (2011). *On Privacy*. London: Routledge.

Louis Harris Associates, and A. Westin (1990). *The Equifax report on consumers in the information age*. Atlanta, GA: Equifax, Inc.

Mander, W. J., and S. Panagakou (Eds.) (2016). *British idealism and the concept of the self*. London: Palgrave Macmillan.

Mizutani, M., J. Dorsey, and J. H. Moor (2004). The internet and Japanese conception of privacy. *Ethics and Information Technology*, 6(2), 121-128.

Moore, B. (2018). *Privacy: Studies in social and cultural history*. London: Routledge (first published 1984).

Murata, K., and Y. Orito (2008). Rethinking the concept of the right to information privacy: A Japanese perspective. *Journal of Information, Communication and Ethics in Society*, 6(3), 233-245.

Nakada, M., and T. Tamura (2005). Japanese conceptions of privacy: An intercultural perspective. *Ethics and Information Technology*, 7(1), 27–36.

Nippert-Eng, C. E. (2010). *Islands of privacy*. Chicago, IL: University of Chicago Press.

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

O’Brien, D. M. (1979). *Privacy, law, and public policy*. New York, NY: Praeger.

Orwell, G. (1949). *Nineteen eighty-four*. London: Martin Secker & Warburg.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, NC: University of North Carolina Press.

Roessler, B. (2005). *The value of privacy*, trans R. D. V. Glasgow. Cambridge: Polity Press.

Roessler, B., and D. Mokrosinska (Eds.) (2015). *Social dimensions of privacy: Interdisciplinary perspectives*. Cambridge: Cambridge University Press.

Roszak, T. (1994). *The cult of information: A neo-Luddite treatise on high-tech, artificial intelligence, and the true art of thinking*, 2nd ed. Berkeley, CA: University of California Press.

Royal Academy of Engineers (2007). *Dilemmas of privacy and surveillance: Challenges of technological change*. London: The Royal Academy of Engineers.

Schoeman, F. D. (1992). *Privacy and social freedom*. Cambridge: Cambridge University Press.

Sewell, G., and J. R. Barker (2001). Neither good, nor bad, but dangerous: Surveillance as an ethical paradox. *Ethics and Information Technology*, 3(3), 181-194.

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

Surveillance Camera Commissioner (2018). *Annual report 2016/17*. London: Surveillance Camera Commissioner.

Tyler, C. (2017). *Common good politics: British idealism and social justice in the contemporary world*. [n.p.]: Palgrave Macmillan.

van der Geest S. (2018). Privacy from an anthropological perspective. In B. van der Sloot and A. de Groot (Eds.), *The handbook of privacy studies: An interdisciplinary introduction* (pp. 413-443). Amsterdam: Amsterdam University Press.

Vysniauskas, G. (2018). More important than Kant and Hegel. *Logos*, 96. Available at http://www.litlogos.eu/L96/Logos_96_017_027_Vysniauskas.pdf

Waldman, A. E. (2018). *Privacy as trust: Information privacy for an information age*. Cambridge: Cambridge University Press.

Warren, S., and L. Brandeis (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

Westin, A. (1967). *Privacy and freedom*. New York, NY: Ig Publishing.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453.

Alistair S. Duff, PhD, is professor of information policy, School of Arts and Creative Industries, Edinburgh Napier University. A philosophy graduate of the University of London (King’s College), he has tutored at the University of Glasgow and had visiting appointments at the Universities of Zurich and Oxford. The author of *Information Society Studies* (Routledge 2000) and *A Normative Theory of the Information Society* (Routledge 2012), Duff is also a media commentator on privacy and many other information policy issues.

Address: School of Arts and Creative Industries, Edinburgh Napier University, Merchiston campus, 10 Colinton Road, Edinburgh EH10 5DT, Scotland, UK.
a.duff@napier.ac.uk