Ethics and Information Technology (2021) 23:373–383
https://doi.org/10.1007/s10676-021-09580-4

ORIGINAL PAPER

Was Snowden virtuous?

Clive Harfield[1]

Accepted: 18 January 2021 / Published online: 28 January 2021

Abstract
Professor Shannon Vallor's theoretical framework of technomoral virtue ethics identifies character traits that can be cultivated to foster a future worth wanting in an environment of (mostly digital) emerging technologies. Such technologies and increased citizen participation in the new digital environment have reconfigured what is possible in policing and intelligence-gathering more quickly, perhaps, than sober and sensible policy reflection and formulation can keep pace with. Sensational and dramatic, seismic and devastating, the Snowden disclosures represent a particular expression of dissent against American intelligence community exploitation of emerging technologies in undertaking mass surveillance on a global scale. Responses to Snowden's actions, and perceptions of the (dis)value of the disclosures he made, are polarized. Polar opposites equate to vices in the Aristotlean view that posits virtue as the middle way. Here, the theoretical framework of technomoral virtue ethics is used for objective evaluation of Snowden's asserted motivations and documented actions against the benchmark of good cyber-citizenship that the framework describes. The fact that Snowden's account is strongly disputed by the U.S. Government does not in and of itself invalidate a theoretical evaluation. It is not the probative value of Snowden's account that is being tested, but how the narrative presented measures up to an ethical framework.

Keywords Edward Snowden · Emerging technology · Mass surveillance · Technomoral ethics · Virtue ethics · Whistleblower

Introduction

On 20th May 2013 Edward Snowden, employed by Booz Allen Hamilton as a contractor to undertake work for the United States National Security Agency [NSA], departed Hawaii where he was then living and working and flew to Hong Kong. He had in his possession in digitized form a large quantity of files acquired from his workplace (U.S. authorities subsequently claimed it was 1.7 million files: Strohm and Wilber 2014). The files and the information contained therein were classified U.S. government secrets. On the 3rd June 2013 Snowden met with journalists Glenn Greenwald and Laura Poitras at the Hong Kong hotel where he was staying and during the next few days disclosed to the journalists contents of the files he had taken from the NSA (Greenwald 2014; Snowden 2019). Snowden intended that the journalists should publish the content, bringing it to public attention, thereby informing a public debate about mass surveillance of citizens by government which, prior to Snowden's disclosures, was being undertaken without the public's knowledge and in contravention of several constitutional and statutory prohibitions (2019, p. 239).

Snowden's acquisition, removal, and disclosure of the files were unauthorized and in breach of his employment contract. His actions are alleged to be criminal. On the 14th June 2013 the U.S. Department of Justice filed charges against Snowden of theft of government property (18 U.S.C. 641), unauthorized communication (18 U.S.C. 793(d)), and wilful communication of classified communications (128 U.S.C. 798 (a)(3)).[1] On 23rd June 2013, Snowden flew from Hong Kong to Moscow. His passport

✉ Clive Harfield
charfiel@usc.edu.au

[1] Institute for Cyber Investigation and Forensics, University of the Sunshine Coast, Sippy Downs, QLD, Australia

[1] Case No. 1:13 CR 265 (CMH) United States District Court for Eastern District of Virginia. Retrieved from http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/ (accessed 10 April 2020). Title 18 of the U.S. Code, 'Criminals and Criminal Procedure', is accessible at https://www.law.cornell.edu/uscode/text/18/part-I (accessed 10 April 2020).

invalidated by the U.S. government for all international travel except a return to the U.S. (Epstein 2017, p. 106), Snowden remained in Moscow's Sheremetyevo airport for 40 days unable to leave the airport without a valid travel document (Russian authorities asserting that his passport had been cancelled completely: Snowden 2019).[2] Whilst prevented from leaving the airport, Snowden applied to twenty-seven different nations for political asylum (Snowden 2019). All applications were denied. On the 1st August 2013 Snowden was granted temporary asylum by the Russian government. In October 2019 Snowden was granted permanent residency in Russia, renewable every three years. He remains subject to criminal charges in the United States, where President Trump has both called for Snowden's execution (Shapiro 2017) and contemplated pardoning him (Walters 2020).

Information from the files Snowden disclosed was first published in *The Washington Post* and *The Guardian* newspapers on 6th June 2013. Subsequent disclosures were published in *The New York Times*, *Die Spiegel*, *El Pais*, and *La Monde* newspapers in the United States, Germany, Spain, and France. The Australian Broadcasting Company and the Canadian Broadcasting Company also broadcast information obtained from the disclosures. The information thus made publicly available brought to the attention of the world the fact that agencies from the intelligence communities in the United States, the United Kingdom, and Australia (amongst others) had collaborated in unlawful mass surveillance via digital technologies in breach of their citizens' constitutional rights and statutorily-protected human rights, and in breach of laws that expressly prohibited mass surveillance (see, for example, Dorling 2013; Greenberg 2013; Hopkins 2013; Pfister et al 2013; Williams 2013; Gellman 2020). Officials assert that 'Snowden caused tremendous damage to national security' and that 'the full scope of the damage inflicted by Snowden remains unknown' (U. S. House of Representatives 2016, pp. i–ii).[3]

Snowden has been demonized as a traitor (see, for example, Keck 2013; Fletz 2016) and lionized as a hero (see, for example, Cassidy 2013; Giraldi 2013). Taking no sides in the polarized polemic, this paper evaluates the asserted motivations of Edward Snowden against a virtue ethics conceptual benchmark: the taxonomical framework of twelve technomoral virtues proposed by Professor Shannon Vallor (2016).

Edward Snowden could and should have expected that his actions would incur significant adverse consequences and disadvantage to himself. Foreseeable adverse consequences were likely to include moral harms such as social denouncement both informally through the media and formally through court trial if convicted; compounded with material harms such as loss of income and constrained future employment opportunities. Snowden could reasonably have anticipated estrangement of family and friends collaterally disadvantaged because of their association with him; and existing criminal laws in the U.S. and the U.K. mean that any journalists co-operating with the disclosure risk conviction themselves. Snowden fully recognized all this (see, for example, Snowden 2019, pp. 7–8; 242; 260; 262–263; 282; 285; also Scheuerman 2014, p. 610; Epstein 2017, pp. 86; 105; Gellman 2020, p. 254). Yet, certain there would be no good outcome for himself whatever transpired, apparently strongly motivated, Snowden went ahead anyway. Snowden acted to his own obvious and certain disbenefit and detriment.

How and whether Snowden has personally benefitted directly from his disclosures remains a matter of conjecture. Epstein alleges that it is inconceivable that Snowden did not directly benefit: his Russian residence a reward for spying is insinuated (2017, pp. 105–110). Snowden denies this (Gellman 2020, pp. 257, 291, 293, 294); former FBI Director James Comey has stated 'I don't remember seeing evidence either of the Russians having the material or that he [Snowden] was an asset [for the Russians]' (Gellman 2020, p. 334). Snowden has benefitted from having become widely-known through media coverage of the disclosures, and is able to work online, being much in demand for consultancy and speaking engagements (Gellman 2020, p. 320). Nevertheless, income Snowden has earned from his book and from speaking engagements has been forfeited to the U.S. government (Polantz 2020).

Argument can be made that multiple others benefitted from Snowden's actions. Exposure of government agency wrong-doing triggered increased public and political awareness of accountability vulnerabilities, prompting legislation modifications intended to deter or curb further constitutional abuses on the part of government agencies (for example, the U.S. Freedom Act 2015); improved legislation reasonably

[2] Epstein (2017) and Snowden (2019) present different accounts of the circumstances surrounding Snowden's journey from Kong Kong to Moscow and the cancellation of his U.S. passport that cannot be reconciled, and which—for the purpose of this paper—do not need to be.

[3] Claims that lives were lost or would be seriously imperilled by Snowden's actions cannot be verified; no substantive evidence has been made public to substantiate the claims (Scheuerman 2014, p.614; Munro 2018, p.110). By definition if such evidence existed, it would be a classified secret. Ironically, one such claim was made by a senior political figure following a confidential briefing to members of the U.S. Congress House Intelligence Committee, and thus itself an unauthorized leak of classified information (Risen 2014). The unredacted text of the 2016 Congressional Review makes reference only to 'the loss of intelligence streams that saved American lives', (p.i). Former FBI Director James Comey has stated that the U.S. is 'not as bad off as people thought we would be' as a result of the disclosures (Gellman 2020, p. 335).

being regarded as a social and community good.[4,5] Former U.S. Vice-President Al Gore summarised the conundrum of contrasting and conflicting values, observing that Snowden, 'clearly violated the law so you can't say OK, what he did is all right. It's not. But what he revealed in the course of violating important laws included violations of the U.S. constitution that were way more serious than the crimes he committed. In the course of violating important law, he also provided an important service. … Because we did need to know how far this has gone' (MacAskill 2014).[6]

Snowden in journalistic and academic commentary

In 2017 investigative journalist Edward Jay Epstein published an in-depth critique of Snowden's actions. Epstein countered Snowden's self-presentation as a whistle-blower by alleging Snowden was a spy (for Russia, or China, or both, pp. 105–110) whose actions have caused and will continue to cause great damage to America (p. 301). Epstein also identified serious mistakes in America's management of intelligence-gathering (2017, pp. 299–301).[7] Epstein's reasoning has been variously reviewed as 'very persuasive' (Morris 2017); 'gripping and even-handed' (marketing quote attributed to an unnamed *Washington Post* writer); and a 'wobbly souffle of speculation', (Lehmann 2017). Epstein sceptically challenges Snowden's account as it then existed in a portfolio of online and in-print media interviews, but Epstein's analysis exhibits an inclination towards insinuation (two examples on pages 25, 91); a preference for value-laden vocabulary over the language of objective reporting (see pages 34, 39, 44); a reliance on unsupported assumption (see pages 20, 40, 110); and the deprecation of journalists who worked with Snowden (see pages 59, 97); all of which might have been more rigorously edited to avoid conveying an impression of uncritical subjectivity.

Two journalists with whom Snowden collaborated have published their own perspectives (Greenwald 2014; Gellman 2020). In telling their own stories, each took a different approach although both comment on surveillance and society in light of the disclosures. Whereas Greenwald wasted no time in presenting Snowden as 'inspirational' (2014, p. 253), Gellman pondered at length on the nature of his relationship with Snowden, whom he found to be 'fine company: funny and profane, an autodidact with a nimble mind and eclectic interest' but someone who could also be 'stubborn, self-important and a scold' (2020, p. xiii). Gellman, unwilling to engage in the hero/villain 'labelling debate' (2020, p. 333), ever aware that he could be hostage to Snowden's occasional 'instrumental approach to the truth' (2020, p. 324), approached Snowden and government agency officials alike with the same level of forensic scrutiny, as he conveyed—with context—the warning that Snowden wanted the world to hear.

In 2019 Edward Snowden published his own account of the events leading up to his current circumstances, *Permanent Record*.[8] Like Epstein, Snowden writes to convey the message that he wishes to present. In that regard, he should not be read uncritically. Equally, given all that has been written and said about him by others, Snowden is entitled to present his own account. For the purpose of this exercise, the motivations presented in *Permanent Record* (2019) have been taken at face value, but it should be noted that the Congressional Report claims, as of 2016, that 'the public narrative popularized by Snowden and his allies is rife with falsehoods, exaggerations, and crucial omissions' (2016, p. i).

In academic literature Fuchs and Trottier (2017) identified four main themes arising from the disclosures: studies focusing on public opinions about and reactions to Snowden's actions; studies focusing on privacy and surveillance; studies focusing on the extent of internet connectivity; and studies

[4] It is claimed that foreign intelligence services hostile to U.S. interests benefitted from the disclosures—to the extent that such entities had access to the material made public, this is certainly true. Epstein insinuates (2017, p.110) and Snowden denies (2019, p.297) that information from the files which was not made public has been supplied to the Russian intelligence community—in exchange for Russian protection of Snowden from U.S. jurisdiction. There is no independent means of substantiating either this claim or the denial. The 2016 Congressional Review found that Snowden 'did share intelligence' with Russian authorities, based on an unverified claim made by the deputy chairman of the Russian parliament's defence and security committee (p.20).

[5] In the U.K., the Investigatory Powers Act 2016 likewise rendered lawful, intelligence community common mass surveillance practice that previously was unlawful.

[6] The Editorial Board of *The New York Times*, 1st January 2014, made the same point, arguing that Snowden deserved to be treated with clemency as the wider benefits arising from his actions outweighed specific adverse consequences. 'He may have committed a crime to do so, but he has done his country a great service.' Subsequently, in a judgement published 2nd September 2020, a Court held that U.S. agencies had acted unlawfully (in the manner alleged in the Snowden disclosures). The matter before the Court required no determination on whether such collection was also unconstitutional. The Court acknowledged it might be, but made no ruling: *United States v Moalin* No. 13–50,572 (9th Cir. 2020), retrieved from https://cdn.ca9.uscourts.gov/datastore/opinions/2020/09/02/13-50572.pdf, 2nd September 2020.

[7] The fifth finding of the 2016 Congressional Review was that three years after the disclosures, the U.S. intelligence community still had 'not done enough to minimize the risk of another massive unauthorized disclosure', (p. iii).

[8] U.S. authorities promptly filed a civil lawsuit to seize all royalties from the book asserting the book's publication to be in violation of a non-disclosure agreement signed by Snowden as part of his employment conditions: Case 1:19-cv-01197, filed 17th September 2019 in the U.S. District Court for the Eastern District of Virginia, Alexandria Division, accessible online at https://www.justice.gov/usao-edva/press-release/file/1203231/download (accessed 10 April 2020).

focusing on journalism and the public sphere. Lyon added *Surveillance After Snowden* (2015) to his study on *Surveillance After September 11* (2003). Adams et al. (2017) found divergent views on whether other computer systems specialists, finding themselves in a similar position, would emulate Snowden—although their research also evidenced wide consensus that his actions are perceived to have helped rather than harmed society. Johnson (2018), meanwhile, illustrated contrasting attitudes amongst American journalists, juxtaposing the editorial outrage expressed when journalists were subject of legally-sanctioned, albeit secret, surveillance against the muted editorial ambivalence in relation to the unlawful mass surveillance of citizens exposed by Snowden.

There have been various considerations of different morally significant aspects of the Snowden disclosures. Lucas (2014) considered if and when a policy of mass surveillance, undisclosed to the public being surveilled, might ever be morally permissible. Lustgarten (2015) pondered the implications for professionals of ethical digitized retention of psychology and medical patient records. Broeders (2016) argued that an individual's secrets should be protected from exponential digital transparency and that the function of state secrecy, with its emphasis on over-classification, is in need of review and reformulation. Bellaby (2018) suggested that the time has come to make anonymising technology mandatory for all internet users.

Scheuerman reflected upon Snowden's action as a manifestation of civil disobedience, the main function of which 'is to challenge political complacency by bringing public attention to issues that may never have been meaningfully deliberated about in the first place, or where an overdue re-examination of policy is stymied by privileged vested interests and institutional stasis' (2014, p. 615). Such an interpretation is not incompatible with Snowden's definition of a whistleblower (2019, p. 238–239):

> a person who through hard experience has concluded that their life inside an institution has become incompatible with the principles developed in—and the loyalty owed to—the greater society outside it, to which that institution should be accountable. This person knows that they can't remain inside the institution, and knows that the institution can't or won't be dismantled. Reforming the institution might be possible, however, so they blow the whistle and disclose the information to bring public pressure to bear.

How should we think about what Snowden did?

Surveillance has a chilling effect on autonomy and the exercise of agency (Penney 2017; see also Marx 2016, p. 320; Galic et al 2017), particularly in the digital environment where agency can be significantly and insidiously manipulated (Beever et al, 2020, pp. 146–162). The NSA programs disclosed by Snowden sought to 'sniff it all, know it all, collect it all, process it all, exploit it all, partner it all' (NSA classified presentation from 2011, disclosed by Snowden, 2019, p. 222; quoted in Gellman 2020, p. 311). The NSA envisaged a digital environment—for their purposes—devoid of privacy, ostensibly rationalized on the basis that some individuals might use digital technologies for malign purpose, so all users must be viewed with suspicion and surveilled. Snowden dissented: 'I don't want to live in a world where everything I say, everything I do, everyone I talk to, every expression of creativity and love or friendship is recorded.'[9] And so, he acted. Throughout his book, without necessarily expressing himself in terms of theoretical moral philosophy, Snowden discusses matters of moral significance; constructing an ethic amenable to philosophical scrutiny.

Deontological consideration assesses moral worth in terms of the nature of an act. To the extent that Snowden's actions violated his employment contract conditions, the conduct is characterized by dishonesty. If Epstein's analysis of Snowden's career path is correct (2017), Snowden not only violated his duties as defined in his employment contract, he used others as means to achieve his own ends. In that sense, Snowden's actions seem little different in character from the implementation of unconstitutional mass surveillance contrary to law. Furthermore, Snowdon's actions constituted alleged crimes established in laws that are not obviously or entirely morally unsound.

Consequentialist perspectives might be argued either way—politician and public awareness of systemic unlawful practices implemented by government agencies is seemingly in the public interest when such exposure fosters improved governance and consistent adherence to the law (which serves the public interest in preserving rule of law). But if significant damage has been caused to U.S. intelligence-gathering and analytical capabilities, this would be a moral harm to the extent that such damage is contrary to the *public* interest rather than just being contrary to *government agency* interests. (Either way, the public interest in preserving and upholding the rule of law and holding government agencies properly to account would seem to carry greater moral weight because government agency disregard for constitutional protections and evasion of proper governance are seriously detrimental and damaging to the legitimacy of the social institution of government in a liberal democracy. The integrity of this social institution being of fundamental public moral interest.)

[9] Attributed to Edward Snowden on https://edwardsnowden.com, accessed 20th October 2020.

Whether a utilitarian greater good was served depends on who defines 'the greater good', and how. Intelligence community agencies might be expected to construe their methods and operations as being for the 'greater good'—by which lights Snowden's actions were contrary to the greater good, as defined by the intelligence community. But the wider community may perceive matters differently. The fact that 4.5 billion internet-users are now better informed about how they are subjected to mass surveillance and what data about them is being gathered and disseminated between intelligence community partners without user informed consent, arguably outweighs government agency self-defined interests.[10]

But these possible permutations perpetuate polarization. A less contentious approach might be found in virtue ethics; an approach little explored in academic commentary about the Snowden disclosures to date.

Technomoral virtue

Virtue ethics assesses moral worth of *character* rather than of a specific *conduct* or *consequence*. In general terms, a virtuous person is defined here as one who reliably discerns and employs effective means to achieve end(s) in any given circumstance that promote human flourishing (as individuals and in communities); to live well and flourish both as individuals and as communities being regarded as a desirable good (Vallor 2015, 2016). In relation to virtue ethics and use of technology, Professor Shannon Vallor's work provides significant insights, including the identification of technomoral virtues: specific moral character traits that will help individuals and communities alike to live well and flourish in the digital environment.[11]

Archaeology and history provide evidence that with each successive technological era human practices and institutions are re-shaped by emerging technologies. The consequential disruption produces both benefits and disbenefits. On the one hand technology has relieved workers from the tedium of mundane, monotonous work offering little in the way of stimulation; on the other hand, increasing reliance on technology has resulted in deskilling within the workforce. Vallor argues that such deskilling can be moral and as well as practical. 'Moral skills appear just as vulnerable to disruption or devaluation by technology-driven shifts in human practices as are professional or artisanal skills such as machining, shoemaking, or gardening. This is because moral skills are typically acquired in specific practices which, under the right conditions and with sufficient opportunity for repetition, foster the cultivation of practical wisdom and moral habituation that jointly constitute genuine virtue' (Vallor 2015, p. 109). With each new emerging technology therefore—and mindful of nurturing moral skilling whilst avoiding moral de-skilling—there is a need to discover and (re-)define virtue in relation to the use of that technology.

Vallor proposes a framework of technomoral virtues founded upon four premises: cultivating virtuous practices enables individuals and communities to achieve shared goods; the current technological era has given rise to coordinated technosocial practices with their own moral goods; with human life increasingly interconnected and interdependent, human flourishing 'will depend in large part on how effective we become at coordinating our decisions and activities' to secure moral goods; and, to realize such goods 'we will need to begin to cultivate in ourselves that set of moral virtues most likely to foster their realization' (Vallor 2016, p. 51).

Reflecting on the emerging technologies of biomedical enhancement, robotics, artificial intelligence, social media and communications, as well as digital surveillance technologies, Vallor builds on her foundational premises a taxonomy of *technomoral virtues*: honesty; self-control; humility; justice; courage; empathy; care; civility; flexibility; perspective; magnanimity; and technomoral wisdom—with each of which are associated *related virtues* (see Fig. 1).[12] Behaviours and attitudes that—if cultivated to the level of habituation—will enable individuals 'to live well in a world made increasingly more complex and unpredictable by emerging technologies … we need to cultivate in ourselves, collectively, a special kind of moral character', a moral character for the twenty-first century digital environment defined by technomoral virtues (2016, p. 1).

Why these behaviours? Other relevant virtuous traits could reasonably be argued to contribute to technomoral wisdom and technosocial well-being. The principal technomoral virtuous traits identified in Fig. 1 (inner ring), are those regarded by Vallor as the behaviours and attitudes '*most* crucial' to achieving the individual and collective good of living well in the digital environment and with other emerging technologies (2016, p. 120; original

[10] Global internet user statistics retrieved from https://internetworldstats.com/stats.htm, 26th May 2020.

[11] Virtues are cultivated rather than innate. Vallor takes into account Aristotelian, Confucian, and Buddhist constructions of virtue in proposing a pluralistic response to the cultural challenges posed by emerging technologies.

[12] Technomoral wisdom is a different category of virtue from the others in Vallor's framework. Wisdom is a complete virtue rather than a specific excellence or disposition: 'a *general condition* of well-cultivated and integrated moral expertise that expresses successfully—and in an intelligent, informed, and authentic way—each of the other virtues of character that we, individually and collectively, need in order to live well with emerging technologies' (Vallor, 2016, p.154; original emphasis).

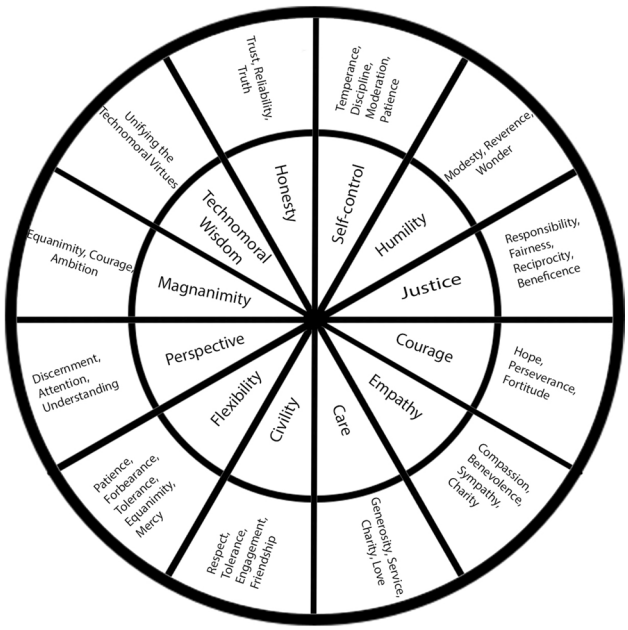

Fig. 1 Vallor's technomoral and related virtues

emphasis—the outer ring of the diagram presents virtues related to the principal technomoral virtues).

The digital environment in which the majority of the global population co-exists alongside the physical environment offers new opportunities for self-expression and self-representation, and to achieve new shared goods: individuals and communities flourishing accordingly, exhibiting and enjoying the benefits of applied technomoral wisdom. Equally the digital environment offers new avenues for morally harmful exploitation ranging from serious crime to tortious intrusion of privacy, with wider ramifications for society beyond each individual victim (see, for example, Bronitt & Gani, 2003; Aiken et al, 2015; Holt et al, 2018). The scale of digital connectivity amplifies benefits and harms.

Cultivating and practising the behaviours identified in Vallor's theoretical framework, it is argued, will facilitate individuals' discernment and employment of effective means to achieve desirable ends, so promoting individual and community well-being within the digital environment. If it can be demonstrated that an individual advocates and adheres to these values, exhibiting aptitude for and application of the exemplary behaviours and traits that are integrated in overarching technomoral wisdom, then that individual can be said to be living virtuously in relation to the use and impact of emerging technologies, including digital surveillance. It is against this proposition for living well and wisely in the evolving environment of emerging digital technologies that Snowden's traits—to the extent that these are apparent from words and actions—are considered.

Snowden through the technomoral virtue lens

Detailed consideration of Snowden's actions/motivations against each of Vallor's twelve technomoral virtues is not feasible within a single paper. The approach adopted here has been to reflect on three such virtues that seem particularly germane in Snowden's case.

Honesty—respect for the truth—with its related virtues of trust, reliability, and integrity, is the first technomoral virtue proposed by Vallor. In the technomoral context, honesty is closely associated with trust: 'honesty is about the appropriate and morally expert communication of information', (Vallor 2016, p. 121). When deception by digital means and indiscriminate covert mass surveillance are so easy to achieve, trust is a particular technomoral problem (Schneier 2018). 'Technomoral honesty is not just a personal concern but a social and political one', argues Vallor (ibid.); cause for concern being no more vividly illustrated than by the dissembling—some might say lying—of U.S. agency officials to those in Congress acting on behalf of the citizenry in trying to hold the agencies to account for agency unlawful mass surveillance (Buttar 2014; Osburn 2019).[13] When citizens suspect that governments are being dishonest, or less than adequately honest, about how technology is being used by government agencies to gather and use data about the citizenry and for what purposes—in other words, acting in an untrustworthy manner—then government credibility is eroded and the legitimacy of otherwise worthwhile enterprises corroded. Consider, for example, citizen resistance to downloading the Australian Government's COVIDSafe app, intended to trace possible pandemic contagion contacts, because of a lack of trust in ambiguous government assurances that the surveillance app would not be used for any other form of surveillance, nor its data aggregated with other data sets for data-mining purposes (see, for instance, Wilson 2020); community resistance arguably resulting in reduced effectiveness (Tonkin 2020). Concerns about dishonest use sit alongside concerns about dishonest content. Cyber-enabled foreign interference, for example, has been identified in 41 elections and seven referenda since 2010 (O'Connor et al, 2020), disinformation being weaponized to influence unduly—and so compromise—democratic processes. U.S. agencies engaged in mass digital surveillance

[13] In March 2013, three months before the Snowden disclosures, then Director of National Intelligence James Clapper, under oath before a Congressional Committee, when asked if the U.S. government was collecting 'any type of data at all on millions or hundreds of millions of Americans', replied 'No, sir. … Not wittingly.' Clapper subsequently explained that he had not understood the question, later changing his explanation to say that he had responded in the 'least untruthful' manner he could think of (Osburn 2019).

were both acting unlawfully and being dishonest about doing so, in this way also debasing democratic values.

In an increasingly digitized information environment, Vallor defines the technomoral virtue of honesty as 'an exemplary respect for truth, along with the practical expertise to express that respect appropriately in technosocial contexts', Vallor (2016, p. 122). Telling the truth to the right people, at the right time, for the right reasons. Does Snowden exemplify this?

Access to evidence of what was happening, coupled with the expertise necessary to interpret that evidence, and the civic awareness to recognise its wider socio-political significance, distinguished Snowden from most digital environment users in 2013 (including those of his colleagues who either gave no thought to the wider socio-political significance of the surveillance programs or were complicit: Snowden 2019, p. 38; 132; 235; 240). This placed Snowden in a unique circumstance of moral agency. He faced a choice—to act or not—that confronted almost no other person.

The narrative arc presented by Snowden describes his transition from working 'for the government' to working 'for the public' (Snowden 2019, p. 1). His point of reference in arriving at the decision to act was the U.S. Constitution—which applies equally in the physical and digital environments—and the protections it provides citizens from unwarranted government intrusion into private life (Snowden 2019, pp. 228–233), as which mass digital surveillance without probable cause would seem to qualify. 'Technologists seeking to report on the systemic misuse of technology must do more than just bring their findings to the public, if the significance of those findings is to be understood. They have a duty to contextualize and explain—to demystify' (Snowden 2019, p. 240): to be honest, in other words.

'It is not only the trait of character and the outward actions of a person that constitute honesty. It is also necessary that the behaviour and the trait of character fit the conditions in which the person finds herself and the action performed is not excessive or deficient' (Beever et al 2020, p. 57). Was Snowden's act of disclosure excessive? Public disclosure of any classified information might be considered 'excessive' by those who would restrict access to such information. But that is a different issue from the consideration of excess in this context. Could Snowden simply have disclosed just enough to demonstrate 'proof of principle' (2019, pp. 249; 289)? Not in these circumstances. Snowden asserts a duty to explain significance through contextualization. He sought not only to demonstrate *what* was happening but also *the scale* of what was happening. Anything less might have been deficient; less than fully honest.

By these lights, Snowden acted honestly qua the global community of digital environment users, but particularly those protected by the U.S. Constitution. Harm was being caused to users of the digital environment because they were subject to unlawful mass digital surveillance. Because users were not aware of being surveilled, they could not make properly informed decisions about how to present themselves and manage their interactions in the digital environment.[14] ('Having nothing to hide' does not constitute consent to surveillance.) Autonomy and dignity are infringed. Dishonesty in the digital environment corrupts the trust upon which the benefits and value of the internet as a tool for communication and dissemination are founded. Users have significant moral interest in others being honest, which brings with it a moral obligation to be honest themselves. In telling digital environment users what was happening, proving the scale of what was happening, and identifying its significance, Snowden exhibited the technomoral virtue of honesty.

That he found himself in the position of lone moral agent in these circumstances engages another of Vallor's technomoral virtues: courage, with its related virtues of hope, perseverance, and fortitude.

Vallor defines courage as 'a reliable disposition toward intelligent fear and hope with respect to the moral and material dangers and opportunities presented by emerging technologies' (2016, p. 131), distinguishing it from another of the proposed technomoral virtues—self-control—by the fact that courage 'necessitates risk and sacrifice', (2016, p. 129). The qualification of reliability emphasises that technomoral courage is evident from habit and practice rather than in one-off acts. 'The courageous agent is willing to endure some injury, forgo some legitimate good, or otherwise incur a real loss in order to do what is necessary and right', (2016, p. 129). Added nuance is drawn from the Confucian philosopher Mengzi (fourth century BCE): individuals who fail to recognise the threat to their own dignity posed by living in ethically compromised ways and who consequently fail to care habitually for their self-respect and moral dignity, lack and fail to practise moral courage (Vallor 2016, pp. 130–131). Did Snowden exhibit moral courage?

Snowden understood that he risked social denouncement, likely loss of income, retribution within the context of his career, criminal conviction, and state sanction if he implemented his plans. He recognized that he would endure some injury in consequence of acting. Social denouncement he has suffered; conviction and sanction may yet happen.[15] Had his employment not been terminated for him, Snowden

[14] That someone thus harmed is not aware of being harmed, does not negate the harm. Being unjustifiably surveilled (subject to privacy intrusion) and not being made aware of being surveilled (subject to misuse of government coercive power) are separate harms.

[15] Gellman notes that neither Snowden nor the U.S. government have any appetite—or, indeed, need—for final resolution (2020, 353).

would have had to resign since continuing to work for the NSA would amount to complicity in conduct he argued was unlawful.

Snowden continues to forego legitimate goods. He was on his way to Ecuador when he became marooned in Russia where he eventually had few other options but to seek asylum.[16] To the extent that he is unable to travel freely elsewhere, Snowden is denied the ability to exercise fully the legitimate good of autonomy: it was not his choice to go to Russia, it was his choice to go to Ecuador. Modern communications do not deny him contact with his family and friends still living in the U.S. but, effectively being in exile, he is denied the quality of association with family and friends that he might otherwise have enjoyed. The legitimate good of freedom of association is thus severely restricted.[17] Whilst Snowden is able to make a living, and so support himself, his circumstances constrain his available options for making the best living for himself that he might have chosen had he not acted as he did. All things being equal, freedom of choice is a legitimate good that Snowden is denied; paradoxically because of a choice he made.

Snowden did not have to suffer these harms. He could have avoided doing so, by not saying anything. To benefit others, he chose to place himself in harm's way. This was a one-off act—arguably a rare moment requiring momentary bravery rather than persistent courage as Vallor conceives it (2016, p. 129)—but to be prepared to withstand the likely permanent adverse consequences that Snowden would reasonably have foreseen requires hope, perseverance, and fortitude; the associated virtues Vallor identifies as related to moral courage. In terms of moral courage, so far so virtuous. Other aspects require consideration, however.

Cowardice and recklessness/rashness are the vicious extremes between which the virtue of courage is posited. Has Snowden exhibited either of these vices? Here the longitudinal notions of persistency and consistency are engaged; notions that make manifest Vallor's defining characteristic of enduring reliability in technomoral virtue. Snowden's methodical approach to the disclosures he made (attested by Epstein, Greenwald, and Gellman) can hardly be considered rash. Snowden worked consistently towards his objective over a period of time, persistent in the moral courage needed to confront the personal adverse consequences of the task upon which he had set out. That he was prepared to endure lasting significant personal disadvantage can hardly be considered an act of cowardice. But subsequently argument can be made that in not presenting himself to the jurisdiction of the U.S. to answer the criminal charges he faces, Snowden is exhibiting moral cowardice by appearing to be unwilling to be held to account. That he is placing himself beyond the reach of the rule of law, whilst justifying his own actions in terms of exposing others to account for their disregard—as he sees it—of the law and constitution.

An alternative interpretation might view surrender to U.S. authorities as the opposite vice—rashness. Given that a fickle and unashamedly populist President has, from time to time, demanded Snowden's execution, and that sizeable sections of the U.S. community now agree that the time will come when they need to 'take the law into their own hands' (Bartels 2020, p. 1), thus demonstrating an elastic commitment to the rule of law within the community from which a jury might be drawn, serious questions can reasonably be raised about the likelihood of Snowden being afforded a fair and impartial trial. To surrender himself without such a guarantee could be considered reckless given that his life might be at stake.[18]

Equally, it can be argued that in his current role as president of the board of directors of the Freedom of the Press Foundation, and in the online presentations he continues to deliver from Russia, Snowden is demonstrating consistency—a reliable tendency or disposition in Vallor's terms (2016, p. 131)—with the moral convictions that motivated his actions in 2013, and is therefore exhibiting consistency with desirable traits identified in Vallor's framework.

Noting that the absence of technomoral justice is a destabilising social phenomenon in which mass digital surveillance and data-mining amplify asymmetries of power, Vallor offers a two-part definition for the third element of her taxonomy under consideration here, justice, or the upholding of right: 'a reliable disposition to seek a fair and equitable distribution of the benefits and risks of emerging technologies'; and, 'concern for how emerging technologies impact the basic rights, dignity, or welfare of individuals and groups', (2016, p. 128). Snowden's disclosures alerted digital environment users to hitherto unsuspected surveillance vulnerabilities (and therefore to the risk that information so gained could be used to their disadvantage), but it is with the second part of the definition that Snowden's actions particularly resonate.

[16] A boarding pass evidencing intention to travel on to Ecuador is illustrated in Gellman (2020, 307).

[17] Snowden's partner, Lindsay Mills, emigrated to Russia to live with Snowden. There they married (Snowden 2019, 336). Having to leave her home to be in exile with her chosen partner can be argued to be a sacrifice on Mills's part; as a component of the public blackening of Snowden's character, she also has been subject to ad hominin insinuations (Epstein 2017, 41).

[18] As the law currently stands, Snowden would not be allowed to mount a defence to some of the charges he faces (2019, 293). To address this due process deficiency, an amendment to the U.S. Espionage Act has been proposed to create a public interest defence (Gosztola 2020).

For the lay reader Snowden explicates the intelligence community's 'bulk collection' (2019, pp.172–180)—digital 'mass surveillance' synonymously explains the purpose—before illustrating how intrusive against individual privacy is such data harvesting (see, for example, pp. 194; 208). The importance of privacy (control over information about self) in sustaining personal dignity and in managing personal relationships has been asserted by Rachels (1975). More recently and in wider context Nissenbaum goes further (2010), proposing a 'framework of contextual integrity' to ensure that information is collected, protected, and distributed according to defined norms governing distinct social contexts. Birrer (2005), argues that it is how accumulated data is used that gives rise to the most significant ethical concerns. Marx (2016) discusses similar concerns and notes the complexity of applying ethical standards in modern surveillance. So, Snowden is not alone in voicing the concerns he raises about how new technologies and the uses to which they are put adversely impact the basic rights and dignity, and welfare of individuals and groups (whether or not such uses are those originally envisaged).[19] Practitioner rather than academic philosopher, Snowden found himself confronted with an unavoidable decision to do something or to do nothing, either course having profound wider implications for digital environment users. If he was to act justly—not with favouritism or to inflict injustice (the vicious opposites of justice)—Snowden's actions had to uphold right.[20] Bok argues that 'those who have assumed a professional responsibility to serve the public interest … have a special obligation not to remain silent about dangers to the public' (1989, p. 221). In blowing the whistle, Snowden acted consistently with that special obligation, alerting digital environment users to ways in which unlawful actions on the part of state agencies were infringing constitutionally protected rights and moral interests that speak directly to respecting individual dignity.[21] By this measure, Snowden's actions can be interpreted as being in accordance with valued character traits promoted in Vallor's technomoral virtue framework.

Where is the harm in virtue?

Deontological and teleological approaches can accommodate the notions of justifiable harm in ways that virtue ethics cannot. Instead of harm as the antithesis of benefit, the antithesis of virtue is vice; virtue occupying the mid-point between contrasting vices as has been illustrated above. Virtue ethics focus on character and personal traits rather than specific conduct and consequence. How, if at all, can harmful consequence, direct or derivative, be reconciled with acting virtuously?

It has been claimed that Snowden 'badly damaged an intelligence system that American presidents have relied on for over six decades' (Epstein 2017, p. 301)[22]; and that, secondarily, his disclosures contributed to 'rampant growth of the public's distrust of the institutions of government in America (Epstein 2017, p. 303).[23] These outcomes are consequences, not necessarily solely or wholly attributable to Snowden, and irrespective of good or bad character. Wrongdoing by state agencies (acting in contravention of relevant laws and constitutions) self-evidently is directly harmful; whereas the act of disclosing such harms cannot reasonably be considered harmful in and of itself, particularly when disclosure achieves goods (compliance with the law; increased public awareness of cybersecurity issues—both beneficial ends towards which technomoral virtuousness should strive). That derivative harms (for example, compromised operations, increased personal risks to operatives) might be triggered from wider awareness of the wrong-doing could complicate considerations. An individual disclosing direct harms may or may not have grounds to anticipate the possibility of (specific, foreseeable) derivative harms. Either way, this is not obviously a strong and overwhelming reason not to act consistently and in accordance with technomoral virtue.[24]

To think in terms of act and consequence—intuitive though it might be with a cause célèbre—confuses consideration of virtue based on character traits. Harmful use of digital technologies is antithetical to living well in the digital environment so many now inhabit. In the context of emerging technologies, including the digital environment, Vallor answers the question 'how does one live well' by identifying a framework of behaviours that—when practised—promote well-being in this context. Elements of this framework, those of particular significance in these circumstances, have been used to reflect upon the Snowden disclosures from the

[19] The literature is too extensive to review adequately within the scope of this paper.

[20] Snowden discusses rights on pages 206–207 (2019).

[21] To what extent commercial entities sub-contracted to undertake work for government agencies do or should prioritise public service interests over pursuit of profit is a debate outside the scope of this paper.

[22] American presidents might have relied on such a system for six decades, but Snowden provided evidence that the system had come to operate in the interests of agencies and the regime, rather than in the interests of the public, which can also be argued to be a harmful outcome.

[23] Though critical of Snowden's character and conduct, Epstein nevertheless identified three beneficial consequences from the disclosures: public awareness of the surveillance leviathan; awareness of the security dangers inherent in the outsourcing of NSA functions; and awareness of the perils to privacy arising from data-collection technologies (2017, 299–300).

[24] Detailed consideration of these moral nuances warrants a separate paper.

perspective of virtue ethics. These reflections do not deny the value of deontological and teleological contributions but serve to offer an additional perspective. The complexity of moral issues arising from the Snowden disclosures adds weight to calls for pluralistic analysis of morally complex and significant circumstances (Ess 2006; Beever et al 2020); wherein lies the potential for further work in this area. Making no contribution to the debate about good or bad *outcome*, this present analysis has shown that, as evidenced by his words and actions during and since the disclosures, Snowden exhibits three important *traits of character* that are consistent with Vallor's technomoral virtue framework.

Acknowledgements I am grateful to the anonymous peer reviewer(s) from whose helpful insights this paper has benefitted; and to Bryn Harfield who produced Fig. 1, his digital illustration skills being superior to my own.

Funding: Not applicable.

Data and material availability All data from publicly published sources.

Compliance with ethical standards

Conflicts of interest: Not applicable.

References

Adams, A., Murata, K., & Palma, A. (2017). Following Snowden: an international survey. *Journal of Information, Communication and Ethics in Society, 15*(3), 336–343.

Aiken, M., McMahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). A consideration of the social impact of cybercrime: examples from hacking, privacy, and child abuse material online. *Contemporary Social Science, 11*(4), 373–391.

Bartels, L. (2020). Ethnic antagonism erodes Republicans' commitment to democracy. *PNAS Latest Articles*. https://doi.org/10.1073/pnas.2007747117

Beever, J., McDaniel, R. & Stanlick, N. (2020). *Understanding Digital Ethics*. Routledge.

Bellaby, R. (2018). Going dark: anonymising technology in cyberspace. *Ethics and Information Technology, 20,* 189–204.

Birrer, F. (2005). Data mining to combat terrorism and the roots of privacy concerns. *Ethics and Information Technology, 7,* 211–220.

Bok, S. (1989). *Secrets: On the Ethics of Concealment and Revelation*. Vintage Books.

Broeders, D. (2016). The secret in the information society. *Philosophy and Technology, 29,* 293–305.

Bronitt, S., & Gani, M. (2003). Shifting boundaries of cybercrime: from computer hacking to cyber-terrorism. *Criminal Law Journal, 27,* 303–321.

Buttar, S. (2014). Beyond CIA and NSA spying: corruption. *The Huffington Post*, 19 March 2014. Retrieved May 4, 2020, from https://www.huffpost.com/entry/beyond-cia-and-nsa-spying-corruption_b_4981558..

Cassidy, J. (2013). Why Snowden is a hero. *The New Yorker*, 10 June 2013. Retrieved May 27, 2020, from https://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero.

Dorling, P., (2013). Australia gets 'deluge' of US secret data, prompting a new data facility. *Sydney Morning Herald*, 13 June 2013. Retrieved April 3, 2020, from https://www.smh.com.au/technology/australia-gets-deluge-of-us-secret-data-prompting-a-new-data-facility-20130612-2o4kf.html.

Editorial Board. (2014). Edward Snowden, whistleblower. *The New York Times*, 1 January 2014. Retrieved May 4, 2020, from https://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?searchResultPosition=10.

Epstein, E. (2017). *How America Lost Its Secrets: Edward Snowden, the Man and the Theft*. Alfred A: Knopf.

Ess, C. (2006). Ethical pluralism and global information ethics. *Ethics and Information Technology, 8*(4), 215–226.

Fletz, F. (2016). Snowden is a traitor and a fraud, period. *National Review*, 16 September 2016. Retrieved April 3, 2020, from https://www.nationalreview.com/2016/09/edward-snowden-report-house-intelligence-committee-not-pardon/.

Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: a critical empirical study of computer experts' attitudes on commercial and state surveillance of the internet and social media. *Journal of Information, Communication and Ethics in Society, 15*(4), 412–444.

Galic, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation. *Philosophy and Technology, 30,* 9–37.

Gellman, B. (2020). *Dark Mirror: Edward Snowden and the Surveillance State*. Bodley Head.

Giraldi, P. (2013). Edward Snowden is no traitor. *The American Conservative*, 16 July 2013. Retrieved April 3, 2020, from https://www.theamericanconservative.com/articles/edward-snowden-is-no-traitor.

Gosztola, K. (2020). Proposed reform to U.S. Espionage Act would create public interest defense. *Consortium News*. 12 October 2020. Retrieved November 1, 2020, from https://consortiumnews.com/2020/10/12/proposed-reform-to-us-espionage-act-would-create-public-interest-defense/

Greenberg, A. (2013). NSA's Verizon spying order specifically targeted American's not foreigners. *Forbes,* 5 June 2013. Retrieved April 3, 2020, from https://www.forbes.com/sites/andygreenberg/2013/06/05/nsas-verizon-spying-order-specifically-targeted-americans-not-foreigners/#5915912238fe.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Hamish Hamilton.

Holt, T., Bossler, A., Siegfried-Spellar, K. (2018). *Cybercrime and Digital Forensics*. Routledge.

Hopkins, N. (2013). UK gathering secret intelligence via covert NSA operation. *The Guardian*, 22 December 2013. Retrieved April 3, 2020, from https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism.

Johnson, C. (2018). A 'massive and unprecedented intrusion': a comparative analysis of American journalistic discourse surrounding three government surveillance scandals. *Digital Journalism, 5*(3), 318–333.

Keck, Z. (2013). Yes, Edward Snowden is a traitor. *The Diplomat*, 21 December 2013. Retrieved April 3, 2020, from https://thediplomat.com/2013/12/yes-edward-snowden-is-a-traitor/

Lehmann, N. (2017). Review of How America Lost Its Secrets by Edward Jay Epstein. *The New York Times*, posted 9 January 2017. Retrieved April 10, 2020, from https://www.nytimes.com/2017/01/09/books/review/is-edward-snowden-a-spy-a-new-book-calls-him-one.html.

Lucas, G. (2014). NSA management directive #424: secrecy and privacy in the aftermath of Edward Snowden. *Ethics and International Affairs, 28*(1), 29–38.

Lustgarten, S. (2015). Emerging ethical threats to client privacy in cloud communication and data storage. *Professional Psychology: Research and Practice, 46*(3), 154–160.

Lyon, D. (2003). *Surveillance After September 11*. Polity Press.
Lyon, D. (2015). *Surveillance After Snowden*. Polity Press.
MacAskill, E. (2014). Edward Snowden's NDSA leaks 'an important service' says Al Gore. *The Guardian*, 10th June 2014. Retrieved April 6, 2020, from https://www.theguardian.com/world/2014/jun/10/edward-snowden-nsa-leaks-important-service-al-gore.
Marx, G. (2016). *Windows into the Soul: Surveillance and Society in an Age of High Technology*. University of Chicago Press.
Morris, E. (2017). Review of How America Lost Its Secrets by Edward Jay Epstein. *BookPage*. Posted January 2020. Retrieved April 10, 2020, from https://bookpage.com/reviews/20784-edward-jay-epstein-retracing-snowdens-steps-nonfiction.
Munro, I. (2018). An interview with Snowden's lawyer: Robert Tibbo on whistleblowing, mass surveillance and human rights activism. *Organization Studies, 25*(1), 106–112.
Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford University Press.
O'Connor, S., Hanson, F., Currey, E., & Beattie, T. (2020). *Cyber-enabled foreign interference in elections and referendums*. Australian Strategic Policy Institute.
Osburn, M. (2019). Four different lies James Clapper told about lying to Congress. *The Federalist*, 6 March 2019. Retrieved May 4, 2020, from https://thefederalist.com/2019/03/06/four-different-lies-james-clapper-told-about-lying-to-congress/.
Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review*, 6(2). https://doi.org/10.14763/2017.2.692
Pfister, R., Poitras, L., Rosenbach, M., Schindler, J., & Stark, H. (2013). German intelligence worked closely with NSA on data surveillance. *Die Speigel*. Retrieved May 26, 2020, from https://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html.
Polantz, K, (2020). Edward Snowden agrees to give up more than $5 million from book and speeches. *CNN*. Retrieved October 20, 2020, from https://edition.cnn.com/2020/09/21/politics/edward-snowden-money-books/index.html.
Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs, 4*(4), 323–333.
Risen, T. (2014). Pentagon report says Snowden's NSA leaks risk lives. *US News & World Report,* 9th January 2014. Retrieved April 3, 2020, from https://www.usnews.com/news/articles/2014/01/09/pentagon-report-says-snowdens-nsa-leaks-risk-lives.
Scheuerman, W. (2014). Whistleblowing as civil disobedience: the case of Edward Snowden. *Philosophy and Social Criticism, 7,* 609–628.
Schneier, B. (2018). *Click Here to Kill Everybody*. Norton.
Shapiro, R. (2017). Donald Trump about Edward Snowden: 'there is still a thing called execution'. *Huffington Post.* 7 December 2017. Retrieved April 3, 2020, from https://www.huffingtonpost.com.au/entry/donald-trump-edward-snowden-execution_n_3489944?ri18n=true.
Snowden, E. (2019). *Permanent Record*. Macmillan.
Strohm, C., & Wilber, D. (2014). Pentagon says Snowden took most U.S. secrets ever: Rogers. *Bloomberg*, 10 January 2014. Retrieved April 3, 2020, from https://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.
Tonkin, C. (2020). Just 17 unique cases found by COVIDSafe app. *Information Age*. 27 October 2020. Retrieved October 30, 2020, from https://ia.acs.org.au/article/2020/just-17-unique-cases-found-by-covidsafe-app.html .
U.S. House of Representatives, (2016). *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden*. (15 September 2016). Washington DC: U.S Congress. Retrieved May 28, 2020, from https://fas.org/irp/congress/2016_rpt/hpsci-snowden.pdf..
Vallor, S. (2015). Moral deskilling and upskilling in a new machine age: reflections on the ambiguous future of character. *Philosophy and Technology, 28,* 107–124.
Vallor, S. (2016). *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*. Oxford University Press.
Walters, J. (2020). Speculation grows over pardon for Edward Snowden after Trump remarks. *The Guardian*. 14 August 2020. Retrieved October 22, 2020, from https://www.theguardian.com/us-news/2020/aug/14/edward-snowden-trump-presidential-pardon-speculation .
Williams, R. (2013). Americans pay GCHQ 100M GBP to spy for them, leaked NSA papers from Edward Snowden claim. *The Independent*, 2 August 2013. Retrieved April 3, 2020, from https://www.independent.co.uk/news/uk/home-news/americans-pay-gchq-100m-to-spy-for-them-leaked-nsa-papers-from-edward-snowden-claim-8743775.html.
Wilson, S. (2020). I'm a privacy expert and I have downloaded the COVIDSafe app. *Sydney Morning Herald*, 4 May 2020. Retrieved May 4, 2020, from https://www.smh.com.au/politics/federal/i-m-a-privacy-expert-and-i-ve-downloaded-the-covidsafe-app-20200503-p54pc6.html.