Cybersecurity, Ethics and Collective Responsibility

Professor Seumas Miller
Charles Sturt University and University of Oxford

Source:

Seumas Miller and Terry Bossomaier *Cyber-security, Ethics and Collective Responsibility* (Oxford University Press, 2024)

I. Cybersecurity and Cyber-safety

- Cybersecurity is not cyber-safety: accidental harm is a safety issue; intended harm is a security issue.
- Culpable negligence; no intention but it is security issue
- Data security: (i) confidentiality of information (e.g. breached by data theft);
- (ii) integrity of information (e.g. breached by unauthorised data changes);
- (iii) availability of information (e.g. breached by unauthorised data destruction or unauthorised encryption (ransomware)

II. Cybersecurity wider than Data Security

- Data security definition too narrow: excludes informational & communicative internet use as means:
- (i) incitement to violence;
- (ii) child sex abuse (on-line grooming);
- (iii) ransomware;
- (iv) defamation;

- (v) computational propaganda (interference in democratic processes)
- (vi) cognitive warfare (informational warfare)
- Definition: Cybersecurity as security of cyberspace

III. Cybersecurity Ethical Principles: Example: Privacy and Encryption

- Privacy is not an absolute right.
- No basic moral right to very strong encryption: empirical conditions in which very strong encryption ought to be legally impermissible, given law enforcement needs
- Very strong/end-to-end encryption morally justified if:
- (i) devices belong to dissidents in authoritarian state;
- (ii) severe threat posed by cyber-criminals so citizens & businesses require devices with very strong encryption
- (iii) other means are sufficient for legitimate law enforcement purposes e.g. the use of bulk metadata, hacking, insertion of snooping devices

IV. Cybersecurity: Example: Social Media & Disinformation, Computational Propaganda

- Cambridge Analytica - firm engaged by Trump campaign – illegitimate access to 50 million Facebook users, incl. US voters
- Machine learning processes to target 'vulnerable' US voters in marginal seats with political advertising?
- Internet Research Agency – linked to Russia – used fake social media accounts to spread disinformation to influence election, e.g. 126 million viewed false/misleading Russian content on Facebook
- Facebook, Twitter etc. are communicative and also to a degree epistemic infrastructure, but more than infrastructure (given they are curators, censors) and flawed epistemic infrastructure (given they use algorithms to promote sensationalistic content, low grade content of 'whales' such as

Trump, and driving motive is to maximise average time spent per day on social media and, therefore, profit from advertisers)

V. Normative-Teleological Account of Institutions

- Normative-teleological theory: institutions are joint enterprises in the service of collective ends of human beings which have as their purpose (collective end), collective goods, e.g. universities collective good of knowledge, police forces collective good of law and order, housing industry an adequate supply of housing of reasonable quality and at a reasonable price, collective good of a forum for public political communication
- Special normative theories, e.g. theory of policing, of universities, of banks, of capital markets, of technology companies such as Meta (Facebook), Twitter (X), Alphabet (Google), Nvidia.

VI. Epistemic Institutions

- Notions of collective knowledge (propositional and practical i.e. knowledge how) understood as the principal and ultimate collective end(s) of an institution – might distinguish essentially epistemic institutions from essentially non-epistemic ones.
- Toyota Corporation is not an essentially epistemic institution, notwithstanding that it undertakes research into electric cars, because its principal and ultimate collective end is the production of cars, not knowledge about cars.
- University which conducts research into electric cars remains an essentially epistemic institution if it stops short of producing cars (other than to demonstrate how this can be done, i.e., its research yields knowledge-how).
- Are/ought Facebook, Twitter be epistemic institutions or platforms for epistemic institutions/epistemic interaction akin to Internet service

provider/phone company? If so, in what sense, given Facebook claims to be platform not publisher?

VII. Global Technology Companies

- General principles: (1) Public interest in liberal democracies in efficient, effective channels of public political communication accessible to all i.e. collective good of public forum for political communication; (2) Compliance with norms of evidence-based truth-telling; (3) Public forum & truth-telling norm compliance overrides private commercial interests
- Global technology companies, e.g. Facebook, Twitter) if market-based, must comply with principles free and fair competition; downsized, remove power imbalances, e.g. user pays to replace 'free' access in return for data.
- 'Big Tech', if infrastructure providers, e.g. collective good of public forum, then redesign e.g. public owned utilities, different algorithms.
- (1) social media companies are not epistemic institutions if only goal is to provide infrastructure for content they have no interest in or control over, e.g. akin to phone companies; (2) if social media companies' primary goal is to maximise user hours per day (in order to facilitate attention to advertisements) then they are not epistemic institutions, i.e. their goal is not knowledge but rather 'mindless' attention flipping and manipulation by advertisers (or, at best, knowledge of advertised products).

VIII. Social Media Companies: Redesign

- Social media companies are content curators, censors, promoters of sensational; responsibility and ability to regulate content – ought to be legally liable, e.g. legal status of publishers liable for defamation, incitement etc.
- Licensing of mass social media social platforms conditional on legal compliance e.g. removal of illegal content.

- Account holders with Twitter, Facebook etc. legally required to be registered with independent statutory authority e.g. Office of e-Safety Commissioner, issues unique identifier based on driver's licence etc.
- News/comment on political matters needs to be comprehensive, objective, truthful and evidence-based and, at times, complex
- Redesign: Platform for news media organisations (editors independent of owners, professional journalists) and universities (academic freedom) mandatory, independent, structural element of social media - liable for their own content
- Social media as hybrid institutions: current role AND public political communication 'forum' with inter alia licensed content providers, e.g. news media organisations, universities (financed by social media companies advertising)

IX. Cybersecurity: Example: Cognitive Warfare

- Cognitive warfare emerged from prior non-kinetic forms of warfare, such as PsyOps operations and Information Warfare; Cogntive warfare relies heavily on new communication and information technologies, notably AI, and techniques of psychological manipulation
- "Cognitive Warfare is a strategy that focuses on altering how a target population thinks – and through that how it acts" (Backes and Swab)
- "the weaponization of public opinion, by an external entity, for the purpose of (1) influencing public and governmental policy and (2) destabilizing public institutions" (Nato Report)

X. Cognitive Warfare: Examples

- External Warfare: (i) Russian state interference in US elections - Cambridge Analytica; (ii) Ukraine invasion/propaganda via *Sputnik*, *Russia Today*

- Internal Warfare: (i) Chinese state against Uighurs, Hong Kong democrats i.e. its own citizens
- (ii) Non-state actors engaged in messy, unsystematic, uncontrolled form of cognitive 'warfare' or conflict?: Trump and US right-wing versus US left-wing: polarisation, undermining of liberal democratic institutions?

XI. Disinformation, Propaganda and Social Media

- Social media platforms, Facebook, Twitter etc. used by billions of communicators world-wide, as are search engines, such as Google.
- Internet and social media have also led via echo chambers and filter bubbles to exponential increase in disinformation & political propaganda, e.g. Trump 32,000 falsehoods
- Information warfare use fake accounts, bots to amplify messages and trolling, denial of service attacks, to shut down oppositional communications.
- Empowered extremist political groups, conspiracy theories, (e.g. Islamic State, QAnon), facilitated interference in democratic process by foreign powers (e.g. Cambridge Analytica) and undermined democratic institutions internally, e.g. attack on Congress

XII. Interpersonal Freedom of Speech and Mass Media Channels of Communication

- Distinguish micro-level interpersonal speech, e.g. John Brown speaking to Mary Smith on a street corner, from macro-level socially-directed speech on public policy to millions via mass media channels of public communication, e.g. CNN, Trump on Twitter.
- Access to mass media channels of public communication is necessarily highly restricted and in respect of public policy issues governed by procedures some of which are questionable, e.g. likely to generate profits

XIII. Freedom of Social-directed Speech on Mass Media Channels: Rights?

- Moral right of citizen, A, qua member of his/her political community to speak to the- rest-of A's political community; foreign state actors do not have this right, e.g. Russian state actors do not re US citizens.
- Joint right of members of a political community qua members of that community to listen to foreign speakers via mass media channels of public communication, e.g. foreign state actors or not to do so
- Joint right to ban foreign state actors from communicating to members of liberal democracies via mass media channels of public communication, incl. social media.
- NB: Consistent with micro-level interpersonal right of each member of a community to listen to foreign state actors via channels of communication that are not mass media channels of public communication.
- Recommendation 1: Russian and China state actors' accounts with Facebook, Twitter and other 'big tech' should be revoked (David Sloss), given engaged in cognitive war with liberal democratic states

XIV. Social Media and Freedom of Speech

- Prior to social media, access to the channels of public communication in large representative democracies mediated by the press, e.g. TV, radio, newspapers
- Press regulated, including quality control: editorial independence of government and of ownership, professionalization of journalists, publishers and journalists not anonymous and liable for illegality, e.g. defamation, incitement, pervert justice
- Social media enables speakers, qua individuals and qua members of groups, e.g. QAnon to communicate directly via channels of public communication, i.e. without the press as a mediator, but largely unregulated
- Recommendation 2 (see above): Social media monopoly/oligopolist should have legal liability for enabling communication of content

- Recommendation 3 (see above): Social media monopoly/oligopolist should operate under a licence held conditionally on compliance with minimum epistemic and moral standards, e.g. re trolling.
- Recommendation 4 (see above): News media organisations/universities mandatory, independent, structural element of social media and liable for their content

XV. Right to Amplify Communications?

- No moral right to amplify by following means:
- Amplify by automation, e.g. bots
- Amplify by multiple individuals operating under single direction, e.g. Chinese
- Amplify by deception, e.g. using fake accounts
- Amplify by manipulation, e.g. using bulk data and algorithms to micro-target unknowing 'vulnerable' individuals
- Recommendation 5: Content which is otherwise legal but which fails to meet minimum epistemic standards, e.g., is demonstrably false, AND is significantly amplified by one of above means, is liable to removal in accordance with determination of independent fact-checking authority

XVI. Communicator's Right of Anonymity?

- Privacy is not anonymity; an anonymous communicator is not simply exercising a right to privacy, e.g. right to be left alone.
- In liberal democracies influential communicators (whether originators or amplifiers) of socially directed content on matters of public policy using mass media channels of public communication do not have a basic right to anonymity

- Some influential communicators of socially directed political content using mass media channels of public communication do have a derived moral right to anonymity, e.g. dissidents using social media in an authoritarian state need to be anonymous to avoid arrest/torture

XVII. Reduce Anonymity and Automation

- Recommendation 6 (see above): In liberal democracies account holders (incl. organisations), with mass social media platforms, such as Twitter, Facebook, must register with independent statutory authority e.g. Office of e-Safety Commissioner, which issues unique identifier based on driver's licence etc.
- US etc. social media platforms are required by law only to provide accounts to those who have registered with some statutory authority
- Access under warrant by law enforcement to identity of those who breach laws. No anonymity for lawbreakers
- Botnets cannot use fake accounts. No fake accounts
- Recommendation 7: Frequent communicators of socially directed content on matters of public policy using mass media channels of public communication who have very large audiences, e.g. 100,000 followers, must be publicly identified. No right of anonymity for influential communicators on matters of public policy. NB: This would not apply to one-off communications, e.g. scientific, scholarly or literary works