A privacy impact assessment of the original Gmail, using an ethical framework analysis

*Submitted in partial fulfillment of ZBU6505

Paul John Cronin
Department of Science
University of NSW
Sydney, Australia
p.cronin@student.unsw.edu.au or 0000-0002-4531-1481

***Abstract*—This report evaluates the key legal, regulatory and privacy considerations of Google's original Gmail platform on key stakeholders, with a particular emphasis on data subjects. This evaluation is undertaken using various ethical frameworks.**

***Index Terms*—consequentialism, utilitarianism, deontology, moral rights, justice ethics, care ethics, virtue ethics.**

List of Figures

List of Tables

I. Background

This report evaluates the original data supply chain between Gmail's data subjects, key stakeholders and process owners, including the up and downstream data flows.

A privacy impact assessment of Gmail is required because a data privacy failure could have been an existential level threat to the company.

> "A loss of public trust could end [a] company. Left unchecked, they can permanently damage consumer trust in a brand". [1]

Data security was critical to Google because one of their key differentiators is public trust, to "not be evil" [2].

In 2004, Google launched the Gmail platform:

- providing free email, with an industry-best data security team,
- where all incoming and outgoing emails, from Gmail users and non-Gmail users, were analysed by an artificial intelligence (AI),
- which sold the data for targeted advertisements, and
- there was an upstream flow of all data to the Google ecosystem.

A. Key stakeholders and data subjects

The key stakeholders and their relative power, agency and vulnerabilities can be found in Tables I and II, including:

1) Google, which offered the Gmail platform.
2) Advertisers, who buy access to the Gmail user's data to advertise relevant products.
3) The primary data subjects, the Gmail and non-Gmail users, who sent and received emails through the Gmail platform. Other data subjects were members of the public whose information was contained in processed emails.
4) World governments, who were informed of their citizen's illicit pornography, and who often wish access to data subjects' emails.

To understand the data flows between the stakeholders, see Figure 1 which shows how the data was collected, used, consumed and sold.

B. Purpose of data collection

The purpose of collecting the email data from both the Gmail and non-Gmail users was to profit from its sale to advertisers. It was also stored indefinitely for future Google business activities.

C. Volume, variety, and sensitivity of the data

The statistics for Gmail were phenomenal [3], with 1.8 billion users worldwide, equating to a 43% email market share in 2020. Approximately 300 billion emails were sent and received daily on the Gmail platform.

The variety and sensitivity of the data, as well as the potential for malignant behaviour, was vast. There is still very little law constraining Google in the US and only ethical and governance constraints prevent disaster.

D. Assumptions and biases

1) The author has had a personal Gmail account since 2004, and has made purchases through the Gmail advertisements.
2) Privacy sensitivity varies between generations, with younger people having a much more relaxed view of online privacy [4].

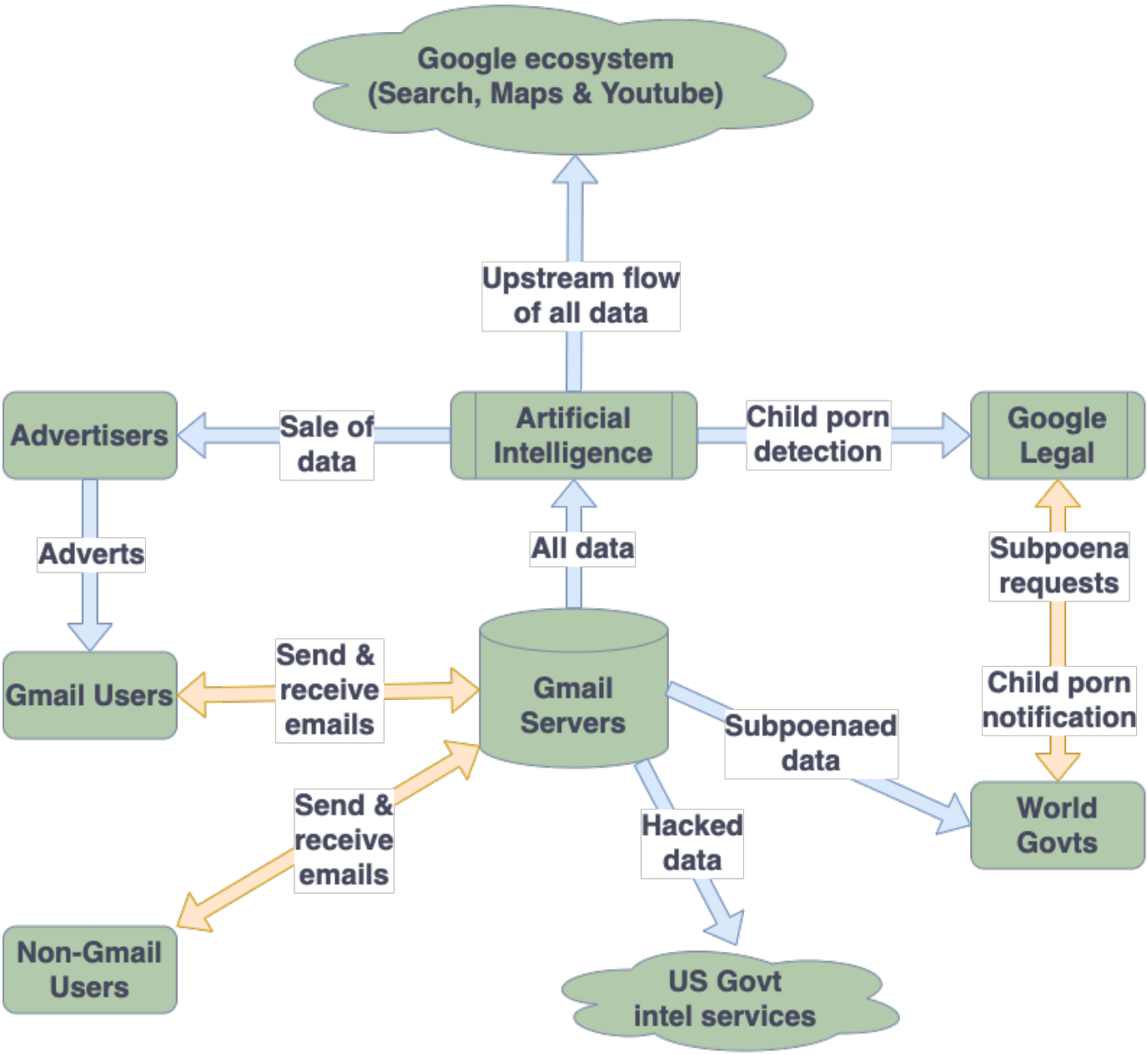

Fig. 1. A simplified outline of the Gmail data supply chain, including key stakeholders and data subjects, as well as the upstream flow to Google and the Google ecosystem.

3) This is a capitalistic world containing advertisements. The Gmail advertisements were tailored for each individual, which could feel disturbing to many.

II. Impacts

It is important to centre the data subjects, and to examine the impacts upon them.

- The privacy of all data subjects' information was impacted, as all data flows upstream to Google where it was collected, analysed and stored indefinitely.
- An unintended impact might not have come till the future. For example, a less ethical Google may have sent targeted advertising emails to non-Gmail users.
- A beneficial impact was for the victims of child pornography. By reporting such instances, criminals were identified and punished.
- An unintended impact could be for political freedoms as Google maintained a secure method for activists to communicate [5].

If we consider stakeholders other than data subjects:

- Gmail became a profitable business, generating $14 billion

Stakeholder (relationship to process owner)	Relative Power	Agency (control of their data)	Vulnerabilities
Google (owner)	Almost total	Almost total as some countries could demand deletions	Profit, good-will, lawsuits
Gmail user (signed up)	Almost none (they could leave)	They could delete their account, but the data was not deleted from Google.	Hacking, subpoenas, loss of privacy
Non-Gmail user (no relationship)	None	Almost none - in some countries they could request their data deleted	Hacking, loss of privacy
Advertiser (paying client)	Large	They profit from the data of others, so did have agency.	A small chance of criticism.
US Govt	Relatively large	Have quite a lot of control under legislation.	Corporate lobbying.
Malevolent Govt	Relatively minor	Have very little power to access their data	Loss of control over citizens

TABLE I
TABLE OF STAKEHOLDERS.

Stakeholder A (greater power)	Stakeholder B (lesser power)	Conflict
Google (owner)	Gmail user	Multiple privacy violations, their data collected, stored and used by Google for future business projects.
Google (owner)	Non-Gmail user	They did not give informed consent to have their information collected.
Google (owner) Advertiser	Member of public Gmail user	Their incidental information in an email may be collected, stored and used by Google without their consent. were shown advertisements based around their private information.
Governments	Gmail user, non-Gmail user, member of public	When a Government may have a legitimate reason to subpoena a Gmail user, others personal data may be exposed too, people who were not Gmail users, and did not give consent.

TABLE II
CONFLICT TABLE BETWEEN STAKEHOLDERS.

in 2014 [6].
- Gmail use has allowed billions of people to communicate, start businesses and obtain an education.

These impacts will have lasting effects on stakeholders.

III. ETHICAL FRAMEWORKS

Ethical relativism argues that right and wrong are relative, depending upon culture, upbringing and workplace, but in a desire for societies to function and flourish [7]. However, it is important that we are ethical pluralists, rather than simply ethical relativists, and as such will examine the data supply chain from various ethical frameworks.

Data should be treated ethically throughout the supply chain. Gmail ethical concerns are summarized here under various frameworks:

A. Consequentialism

Consequentialism asks us to weight alternatives, such as other free or private email services, but the excellent service and security of Gmail is now a taken-for-granted "good" and has made the platform almost ubiquitous.

Consequentialism is one of our dominant mental models, where we consider the consequences of actions and impacts on stakeholders [7]. If we consider the intended and unintended consequences for the data subjects, those being the Gmail and non-Gmail users, who exchange emails through the Gmail platform, we find:

- 1.5 Billion users in 2018, given access to a highly secure communication mechanism.
- Billions of targeted ads that had more efficiently helped companies sell their products.
- Very few, if any, mass privacy failures, unlike other major platforms.
- An unintended consequence was for the non-Gmail users who send or receive and email from a Gmail user. Those non-Gmail users had not given consent to had their emails scanned by Google or had their data used for their profit [8].

Another element of consequentialism is to weight up and consider alternatives. There were plenty of alternatives to Gmail, including free emails services (that also had non-tailored advertisements), and private email servers (which had no advertisements at all).

These services had the drawbacks of not having the industry's best security system and had been hacked, unlike Gmail. Private email servers can had prohibitive financial and expertise costs. The ubiquity of Gmail is now a taken-for-granted as "good". It had an excellent reputation, despite privacy considerations.

B. Utilitarianism

Gmail is an excellent example of Utilitarianism, as it provides a great good for a great number of people. It would be hard to quantify its net benefit, allowing billions of people access to communications that would be otherwise unaffordable.

Utilitarianism seeks the greatest utility, to experience pleasure, and enjoy a shared benefit, while minimizing any social costs or pain. While Gmail had made billions for Google, it would be hard to quantify the net benefit to the world of society

– allowing those access to communications that would have otherwise be denied.

Gmail is perhaps a perfect example of Utilitarianism, that is, it provides a great good for a great number of people. Utilitarianism is often criticized for the rights of minorities are sacrificed - in this case, those non-Gmail users whose information was scanned by the Gmail AI.

C. Deontology

Deontology [9] uses rules to distinguish right from wrong, but can lead us to disregard the possible consequences of our actions. Under this framework, we understand Gmail did not contravene any laws, but its use did have consequences for the data subjects.

Gmail fails under Deontology because people should be treated as ends in themselves, not means to an end. While Gmail supplies a free service, that had contributed greatly to society, the data subjects were a means to an end, that end being to profit from their data.

Deontology advocates for non-maleficence: do not harm. Gmail did very little harm, if you accept that the artificial intelligence scanning emails was harmless. Further, it had a beneficence, that was to proactively do good, by reporting child pornography to the relevant legal authorities.

D. Moral Rights

Moral rights are about what you are entitled to because of your humanness and are a form of deontology. These are separate to, and often proceed legal rights. Gmail was challenged when examined through a moral rights lens, especially when it comes to privacy.

Privacy is a negative right – it is incumbent upon others not to impinge upon an individual's privacy. Privacy means freedom from scrutiny and from exploitation. The data subjects, Gmail users and non-Gmail users, both had their data heavily scrutinized and exploited. This was a greater violation for the non-Gmail user, who was not afforded the opportunity to consent.

Privacy means to had control about what others know about you, but here Google knows almost everything about both the Gmail user and the non-Gmail user, and was willing to sell that information for its profit.

Moral rights require data subjects to know how their data is going to be used in the future. While Google used the data immediately for advertising, it also retains that data, and could exploit it in any way they wish in the future, in ways they might not know originally. This was a clear violation of the moral rights of the data subjects.

E. Justice ethics

There are three forms of Justice Ethics: distributive, procedural and interactional. Under distributive justice, Gmail provides the poorest people access to a platform that would otherwise be out of their financial reach. However, under procedural and interactional justice, Gmail fails as it did not include data subjects in its decision making, nor allow them control of their data.

If we examine the Gmail platform through Justice ethics [10], another form of deontology, we find in many ways it was successful. Amartya Sen said

"Justice is the capability to live a life that's valuable, not just how much resources you have access to".

If we consider distributive justice, where we evaluate outcomes and look at the benefits, equities and rewards derived, then Gmail was a tremendous success. It provides for the poorest people on the planet access to a platform that would otherwise be out of their financial reach.

If we consider John Rawls's "veil of ignorance", we likewise consider Gmail ethically just. Irrespective of the conditions of your birth, your skin colour, your origin, your wealth, you too had access to the same platform as the most privileged members of society.

However, if we consider procedural justice or interactional justice, then Gmail starts to fail. This was because Gmail did not include data subjects in its decision making, they did not participate in the process, nor had access to their own data. The power disparity was incredibly large, without there being a fair relationship. It was "Google's way or the highway".

F. Virtue ethics

When considering Virtue Ethics, Google invests in an industry-best team to protect the integrity and confidentiality of the data and goes out of its way to report child pornography.

From the very early days of Google, they differentiated themselves from other major companies with the motto "don't be evil". This phrase, a declaration of their virtue, was created by Paul Buchheit, who was also the lead developer of Gmail [2].

It's difficult to talk about the virtues of such a megacompany, what makes it a "good" company. Google may not had an "excess of virtues", but they did have an "absence of vices". Given the extraordinary amount of information they had collected upon all Gmail users and non-Gmail users who interact on their platform, they could have "monetized" that information more than by simply selling anonymized data to advertisers. In that manner, Gmail had integrity.

The Gmail platform did protect their members from harm. They did so by investing in the industry best security team, to protect the confidentiality and integrity of the data. This was an expensive investment that other similarly situated companies had not made. This investment was a virtue.

The Gmail platform did assist in human flourishing, another goal of virtue ethics, by allowing communication from any point in the world to any other point, with a minimum of cost or skill.

G. Care ethics

Under Care ethics, Gmail empowers people by providing an amazing service for free, but fails in not seeing the person as an individual. The artificial intelligence that scans the emails did not consider the data subjects as real people, nor did it care about the details of their existence, nor had moral awareness.

Risk	Stakeholders	Likelihood of harm	Severity of harm	Overall risk
Hacking by malignant entity (Government, company, individual)	Google, Gmail users, non-Gmail users	Remote	SEVERE (loss of reputation, lawsuits, loss of customers)	MEDIUM
Malignant governmental subpoena of activist	Non-Gmail users, or member of the public in email	Possible	SEVERE (the possible arrest, torture or death of a user)	HIGH
US Government hacking	Google, Gmail users, non-Gmail users	Possible	Significant (embarrassment to Google, loss of user base)	MEDIUM
Loss of reputation from privacy policy change	Google	Possible	Significant (could go the way of other former virtuous companies).	MEDIUM
Undetected criminal activity	Google, members of the public	Probable	Significant (murder, rape, theft, etc)	HIGH

TABLE III
RISK TABLE - DESCRIBES SOURCE OF RISK AND NATURE OF POTENTIAL IMPACT ON INDIVIDUALS.

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk
External hacking (by corporations, governments or individuals)	Maintain an industry-leading team to ensure that data subjects data remains secure. Divide the data between multiple physical locations.	Significantly reduced, but not eliminated	Google must prevent every attack; the hackers need to succeed once.
Malignant governmental subpoena of activist	Examine on a case-by-case basis by Google Legal in that legal jurisdiction	Significantly reduced	There was a vagueness in regard what was a malignant government and activist.
Loss of reputation from privacy policy change	Maintain high ethical governance structures	Reduced	This was a risk to be managed by good governance
Undetected criminal activity	This was a policy choice to detect and report	Accepted	This policy choice may be changed in the future.

TABLE IV
RISK REDUCTION TABLE - THIS TABLE IDENTIFIES ADDITIONAL MEASURES GOOGLE COULD TAKE TO REDUCE OR ELIMINATE IDENTIFIED RISKS.

The overall aim of care ethics is to empower and emancipate people [11]. Gmail succeeded at this enormously – providing an amazing service for free. In terms of email communication, it did "take care of them".

Where Gmail starts to fail in relation to care ethics, is that it did not see the person as an individual, rather it is dispassionate and impartial. Each user interacted with an artificial intelligence, rather than with a human intelligence. This AI did not consider the data subjects as real people, nor did it care about the details of their existence. Gmail did not "want to take care of them".

The artificial intelligence had no moral awareness, rather it was programmed to maximise profit for Google by matching the data subject's needs to an advertiser.

IV. REGULATORY, PUBLIC INTEREST CONCERNS

A. Privacy implications

Considering the data subjects, those being the Gmail and non-Gmail users who interact through the Gmail platform:

- their data was extremely well secured within the Google ecosystem,
- there was no expectation of privacy within that ecosystem,
- their data, anonymized, was sold to the highest third-party bidder.

B. Regulatory concerns

Google is a US company, so falls under the Electronic Communications Privacy Act (1986) and Patriot Act (2001). In the US, individuals are protected by the Constitution's Fourth Amendment, which prohibits "unreasonable search and seizure".

Google requires a search warrant before supplying the contents of emails, except for imminent dangers, such as to prevent death or serious physical harm [12].

Other legal jurisdictions make demands upon Google, such as Terrorism Act or the Regulation of Investigatory Powers Act (RIPA) in the UK.

Google had a financial interest in both complying with the law and maintaining the privacy of its users, however there was a tension between these legal, ethical and profitability considerations.

C. Public interest concerns

There are several public interests concerns:

1) Only one type of crime (child pornography) was reported to authorities, but not other types, such as planning for terrorism, domestic violence or white-collar crime.
2) It was possible that information about a non-Gmail user could be collected and stored indefinitely by Google, simply by it being contained within an email that passes through the Gmail platform.
3) Google did not hand over political activists in authoritarian jurisdictions [5], but questions had arisen if Google was suffering from ethical decay in exchange for Government contracts [13].

V. RISK PROFILE

This section identifies the top five known and unknown risks, and their impacts, as:

1) Hacking by malignant entities (Government, company, individual),
2) Malignant governmental subpoena of activists,
3) US Government hacking,
4) Loss of reputation from privacy policy change,
5) Undetected criminal activity.

Google made an ethical choice to heavily invest in an industry-best team and hardware to protect the security of user's data. Many companies did not make such investments.

Trust in the Gmail platform comes from their philosophy of "don't be evil" [2].That policy might change to exploit their data assets in a less benign manner.

Gmail only reports one type of criminality on the platform: child pornography. There was no reason that they could not detect a much greater degree of criminality.

Table IV proposes mitigation strategies to reduce risk, especially by maintaining data and corporate governance. None of the risk could be truly eliminated, rather it becomes an ongoing task of managing risk to build trust and collaboration with stakeholders, especially the data subjects.

Non-compliance with regulatory requirements was not considered a credible risk.

VI. Overall recommendation

This report evaluates the consequences and key legal, regulatory and privacy considerations of the Gmail platform on key stakeholders, with a particular emphasis on data subjects' privacy.

This report asses that there are no violations of legal privacy regulations, in fact, Google's lobbying efforts will ensure their voice was always heard.

While this report touches upon many positive ethical aspects of the Gmail platform, including Consequentialism, Utilitarianism and Virtue Ethics, there were real ethical challenges, especially that of privacy.

There were real risks associated with the collection, use and storage of such a vast quantity of data, and this report outlines ways those risks can be minimized.

Unlike other assessments of the Gmail platform, this is a Privacy Impact Assessment report and has identified serious structural failures under Deontology, Moral Rights, Justice Ethics and Care Ethics.

Hence, the Gmail platform, while it had many virtues, was inherently unethical and fails this assessment.

References

[1] Accenture, "Building digital trust: The role of data ethics in the digital age," en, Accenture, Report, Jun. 2016. [Online]. Available: https://apo.org.au/node/71946 (visited on 11/21/2022).

[2] J. Livingston, *Founders at Work: Stories of Startups' Early Days*, en-US, 1st Corrected ed., Corr. 2nd printing edition. 2007. [Online]. Available: https://imusic.co/books/9781590597149/jessica-livingston-2007-founders-at-work-stories-of-startups-early-days-hardcover-book (visited on 11/21/2022).

[3] C. Petrov, *50 gmail statistics to show how big it is in 2020.* en-us, Mar. 2021. [Online]. Available: https://techjury.net/blog/gmail-statistics/ (visited on 11/21/2022).

[4] L. Institute, "The Demographics of Privacy-A Blueprint for Understanding Consumer Perceptions and Behavior," Sep. 2011. [Online]. Available: http://www.laresinstitute.com/wp-content/uploads/2011/09/Demographics-Study.pdf.

[5] M. Wood, *Google offers more secure email for journalists, politicians, activists ... and you?* English, 2018. [Online]. Available: https://podknife.com/podcasts/marketplace-tech.

[6] D. Davila, "Google's 6 Most Profitable Lines of Business (GOOGL)," en, *Investopedia*, 2017. [Online]. Available: https://www.investopedia.com/articles/markets/030416/googles-6-most-profitable-lines-business-googl.asp (visited on 11/21/2022).

[7] T. Wilcox, "Consequentialism and utilitarianism," in *UNSW ZZBU 6505 Course Notes*, UNSW, 2020.

[8] J. Battelle, "Privacy, Gmail, and Unintended Consequences," en-US, *John Battelle's Search Blog*, Apr. 2004. [Online]. Available: https://battellemedia.com/archives/2004/04/privacy_gmail_and_unintended_consequences (visited on 11/21/2022).

[9] T. Wilcox, "Deontology," in *UNSW ZZBU 6505 Course Notes*, UNSW, 2020.

[10] T. Wilcox, "Ethics," in *UNSW ZZBU 6505 Course Notes*, UNSW, 2020.

[11] T. Wilcox, "Care ethics," in *UNSW ZZBU 6505 Course Notes*, UNSW, 2020.

[12] Z. Whittaker, "What Google does when a government requests your data," en, *ZDNET*, Jan. 2013. [Online]. Available: https://www.zdnet.com/article/what-google-does-when-a-government-requests-your-data/ (visited on 11/21/2022).

[13] S. Shane and D. Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," en-US, *The New York Times*, Apr. 2018, ISSN: 0362-4331. [Online]. Available: https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html (visited on 11/21/2022).

Acknowledgment

The author would like to acknowledge Dr Tracy Wilcox, the course instructor for ZZBU6505.