Data Hiders and Finders: Encryption, Profitable Data, and Academic Open Access

A Sociotechnical Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Dylan Cao

May 10, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Dylan Cao

Sociotechnical advisor: Peter Norton, Department of Engineering and Society

Data Hiders and Finders: Encryption, Profitable Data, and Academic Open Access

The International Data Corporation has estimated that by 2018, 33 zettabytes of digital data had been collected worldwide (Reinsel et al., 2018), equivalent to the capacity of about 33 billion mid-sized consumer hard drives at a terabyte each. Americans find data problematic: Pew Research found 81 percent of Americans think the risks outweigh benefits when companies collect data on them (Auxier et al., 2019). Opinions varied greatly by the data use case; 49 percent found it acceptable for underperforming schools to share data to improve student outcomes, but only 25 percent thought that about smart speakers sharing with law enforcement.

Law enforcement groups clash with encryption. Publishers are challenged by the academic open-access movement. Data-based businesses (e.g., Facebook) face privacy concerns from consumers and others. Each of these cases is a conflict between data finders, who seek to use data, and data hiders, who seek to protect it. By comparing these distinct cases, we may find answers about optimizing privacy in the US.

Review of Research

Data is valuable. Contact tracing apps omit useful data (e.g., GPS) to preserve privacy and encourage participation (Fahey & Hino, 2020). Data collecting wearables could help persons with autism read social cues, but issues of consent arise. (Kirkham & Greenhalgh, 2015). One privacy principle is to collect a person's data for their benefit (Van Alstyne & Lenart, 2020). A person is likely to voluntarily share a resume for a job opportunity, but not so they can be psychologically manipulated. This principle is not always applicable; for example, search warrants are allowed despite rarely benefitting their target.

Some specific design rationales fail when directly applied to different fields. Van Alstyne and Lenart's "design for the user" approach (intended for traditional commerce) would suggest that scientific publishers should seek profit primarily, since they control the data. The utilitarian principle behind search warrants (data for the public good) was sacrificed for privacy in COVID tracing (Fahey & Hino, 2020). Despite the challenges, researchers have found ways to borrow privacy principles from other fields. The legal principle of proportionality is the basis of a privacy framework for computing (Iachello & Abowd, 2005). By analyzing different fields, as they did, we may produce useful findings in other fields.

Profitable Data and Consumer Privacy

Profit can be made from either harvesting data or protecting it. Over 98 percent of Facebook's 2019 revenue ($70 billion) came from advertising, which relies on user data (Facebook, 2020a). Apple, in contrast, uses "We're committed to protecting your data" as marketing (Apple, 2021a).

In 2018, Apple CEO Cook said "Our view of privacy started from our values, then we crafted a business plan from that" (Higgins, 2021). Recently, Apple has pursued this aggressively. The next update to iOS will prompt users to opt-in to third-party tracking instead of defaulting to allowing it (Apple, 2021b). Apple has told users in a whitepaper "Some apps request access to more data than is required" and that "companies either face or have paid millions in fines" for abusing user data (Apple, 2021c). It also claims to be the solution to many data privacy issues; for example, "If John had used the Safari browser," it "would have prevented tracking of this activity by default" (Apple, 2021c).

Facebook's CEO Zuckerberg privately said "We need to inflict pain" on Apple and has responded to Apple's actions (Higgins, 2021). In a public blog, Facebook said Apple's new policy is "about profit, not privacy" and is "benefitting big businesses and hurting small businesses" (Facebook, 2020b). In the same post, it believes "Apple is behaving anti-competitively" and commits to providing info to an anti-trust lawsuit against Apple. It has run ads in the *New York Times* and the *Washington Post* to spread its message of "standing up to Apple for small businesses" (Graham, 2020).

In both companies' statements, evidence of their profit rationale is present. Apple wishes to please users and obtain new ones; Facebook wants to maintain its ad effectiveness to support its own clients. Ironically, both accuse the other of using unsavory business practices in the name of profit. However, it is still clear that Apple does regard user consent as essential, while Facebook implies it is following the "design for the user" principle since it says data can "give people better experiences" (Statt, 2021).

Regulatory and Legal Actions

Due to the publicity of these issues, governments have begun to intervene. In 2018, the California Consumer Privacy Act (CCPA) passed to secure "new privacy rights for California consumers" such as the right to request data deletion and the right to opt-out of having one's data sold (California OAG, 2018). A similar bill, the Virginia Consumer Data Protection Act (CDPA) passed the Virginia House and Senate 89-9 and 36-0, respectively, in early 2021 (Virginia LIS, 2021a) (Virginia LIS, 2021b). The CDPA was later signed by the governor (Zakrzewski, 2021). Despite high political support, the Electronic Frontier Foundation (EFF) criticized the VA CDPA since it "has almost no teeth," "stacks the deck against consumers," and does not include a

private right of action, which is the right for individuals to sue over violations (Tsukayama, 2021).

Major privacy bills targeting profitable data have been proposed at a federal level, but none were passed. The Congressional Research Service identified six such bills of the 116th Congress (Gaffney, 2020). Despite each of the bills granting some of the same core privacy rights (such as the right of deletion), Gaffney points to disagreements such as over whether a private right of action should be included as preventing the passage of any privacy bill at a federal level.

Consumer Actions

User actions are not always in line with their thoughts on privacy. Statista reported 223 million US Facebook users in 2020, higher than ever before despite privacy concerns (Tankovska, 2021). Whitehead found that many Facebook deleters "rarely raise political scandals or concerns over data privacy" regarding their reason to leave (Whitehead, 2020). However, users do respond to some changes. In response to a WhatsApp policy change that increased user data sharing with Facebook (Goodin, 2021), interest grew in a non-profit competitor, Signal, to the extent of causing technical difficulties (Signal, 2021).

Law Enforcement and Encryption

Encryption is a data-hiding technique that secures data even from law enforcement. Former Attorney General Barr argued "unlimited privacy" would shield criminals (Barr, 2019b). However, encryption is commonly used in modern devices and internet services.

Non-Criminal Uses of Encryption

Many companies and privacy advocacies deem encryption an essential part of internet and device security. TLS encryption is very commonly used to secure web traffic; according to Google, 95 percent of web requests by Google Chrome in the US used HTTPS and TLS (Google, 2021). Activists may use encrypted messaging such as the Signal app to protect their activities (Nierenberg, 2020). Mozilla implemented encrypted domain name lookups for its US Firefox users (Deckelmann, 2020). The Internet Security Research Group (ISRG)'s "Let's Encrypt" program issued one billion free TLS certificates by 2020, because "Nothing drives adoption like ease of use" (Aas & Gran, 2020). Ecommerce companies heavily depend on encryption to hide data such as payment information. During the second quarter of 2020, ecommerce accounted for about 16 percent of all US retail sales (Commerce, 2020). The Shopify platform added free TLS encryption to its sites as "the right thing for ecommerce in 2016" and sponsors the ISRG Let's Encrypt initiative (Cornu, 2016). Media outlets support encryption to "protect your identity, location, and the information you send us" (New York Times, 2016). Services such as email or cloud storage are also often protected by encryption.

Device manufacturers use encryption to protect device data in cases of physical theft. Most major operating systems offer support: Microsoft Windows offers it as BitLocker, Apple offers it as Data Protection or File Vault for iOS or MacOS, Android has its own "file-based encryption" scheme, and Linux offers the Linux Unified key Setup (LUKS) system. In these systems, not even law enforcement may access the data without the encryption key, leading to incidents such as the San Bernardino court order.

Case Study: The San Bernardino Attack – Apple vs. FBI

In December 2015, a terrorist attack occurred in San Bernardino, California. A perpetrator in the case had an Apple iPhone 5C. A court ordered that Apple assist the FBI in decrypting the phone to obtain "relevant, critical… data" (Blankstein, 2016). Apple objected, arguing it "threatens the security of our customers" and was dangerous to liberty and democracy (Cook, 2016). Apple was widely supported by many tech companies, including Atlassian, GitHub, CloudFlare, Google, Microsoft, Facebook, and Amazon in *amici curiae* briefs (Maddigan & Katyal, 2016; Roth et al., 2016). Maddigan and Katyal asserted that the order "is classic compelled speech," a 1st Amendment violation, by forcing Apple engineers to write code. They also said that the order would "undermine the security of Americans' most sensitive data." Roth et al. argued the order would "erode the core values of privacy, security, and transparency." Maddigan and Katyal stated in the brief that the case was of importance to "customers who trust *amici* to safeguard their data." The companies thus feared that a court decision against Apple would jeopardize trust in their businesses.

Privacy advocacies including the EFF and Electronic Information Privacy Center (EPIC) supported Apple in the matter. EFF's Cardozo said, "I think authoritarian regimes are salivating at the prospect of the FBI winning this order" in an interview (PBS News Hour, 2016). EFF's Buttar noted the FBI's requested tool "would be dangerous" and was "potentially affecting millions of device users" despite the FBI's claims that it was targeting only one device (2016). The EFF filed its own *amicus* brief focusing on alleged 1st Amendment violations, since "The Order forces Apple to say something it does not want to say" (Greene et al., 2016). The EFF's attorneys asserted that the 1st Amendment especially prohibits compelled hypocritical speech, and that forcing Apple to bypass device security would conflict with its messaging on creating

secure phones. EPIC's *amicus* brief primarily argued the order "places at risk millions of cell phone users across the United States" focusing on security concerns unlike the EFF's brief which was more focused on legal concerns (Butler et al., 2016).

The government issued a reply to Apple's motion to dismiss the court order (Decker et al., 2016). In it, the government argued that Apple's "fears are overblown" since the FBI's request required "access to a physical device" instead of attacking network security. They further argued "there is no reason to think that the code Apple writes… will ever leave Apple's possession" and so Apple should be safe to write code to bypass one device's security. The reply also addressed 1st Amendment claims, arguing there is no compelled speech since the court's requirements "leave it open to Apple to decide how to develop the code" and "there is no audience" since the code would remain secret.

Public opinion was deeply divided on the matter. Reuters showed 46 percent supported Apple in refusing to unlock the phone and 35 percent against (Finkle, 2016); CBS found 45 percent supported Apple and 50 percent against (CBS News, 2016); Pew Research Center found 38 percent and 51 percent, respectively (Pew Research Center, 2016). Some did not know who to support. The CBS poll also found that most believed Apple unlocking the phone could set a precedent or make other iPhones vulnerable, despite most of those surveyed by them siding with the FBI. Thus, the security concerns do not prevent some Americans from supporting encryption bypasses. It also appears that campaigns by tech companies and advocacies did not heavily sway the public, at least not immediately.

The court order was eventually dropped when the FBI obtained another way to access the target device (Selyukh, 2016). Thus, no legal precedents were set at over this matter. However,

the incident did demonstrate tech companies and advocacies' abilities to quickly stage massive legal and public communications campaigns over security and privacy issues.

Regulatory and Legal Actions

At present, there is no US federal or state law preventing the use of encryption, but some limits exist on encryption export. Encryption tools can be made publicly available outside the US only after notifying the Bureau of Industry and Security (BIS) and the National Security Agency (Crocker, 2019). Mass market retail products are also eligible for export after approval (BIS, 2017).

Legislation has been proposed to limit the use and capabilities of encryption, but none have received widespread support. As one example, Senators Graham, Cotton, and Blackburn and Representative Wagner introduced the Lawful Access to Encrypted Data Act in June of 2020 (Senate Judiciary Committee, 2020). The act would "bring an end to warrant-proof encryption" by requiring manufacturers to assist law enforcement when presented with a warrant. Senator Graham said encryption hurt prosecution of "numerous terrorism cases" and other crimes. Senator Cotton commented encryption had created a "new, lawless playground of criminal activity." They also cited five specific examples of investigations thwarted by encryption in their press release. Duffie Stone, president of the National District Attorneys Association, said the legislation "represents a realistic path" to addressing encryption (Office of Ann Wagner, 2020). Lawrence Leiser, president of the National Association of Assistant US Attorneys (an organization for federal prosecutors) stated the bill "addresses this gap in enforcement." Privacy advocacies like the EFF called the bill "out of touch with reality," said it disregarded user security, and asked readers to oppose the bill (Crocker, 2019). The Reform Government

Surveillance coalition, representing "big tech" like Google, Amazon, and Apple, objected to the bill as it "would leave all Americans, businesses, and government agencies dangerously exposed to cyber threats" (RGS Coalition, 2020). Despite support from law enforcement and prosecutorial organizations, the Senate version of the bill (S.0451) was not acted on and the House version (H.R.7891) was only referred to committee without further action at this time (Congressional Record, 2020a, 2020b). Some legislation targeting encryption has also been proposed at the state level; for example, California Assembly Bill 1681 would have required smartphones to be decryptable by their manufacturer, but failed (White, 2016).

There have been some attempts by federal legislators to prevent states from passing anti-encryption bills, but these have also failed. Representative Lieu's ENCRYPT Act of 2019 would prohibit states from requiring alterations to software to allow for decryption and would prevent states from banning products due to their use of encryption (Congressional Record, 2019). However, the bill was not acted on after being referred to committee. Overall, recent legislative attempts to limit or further protect encryption have largely failed in the US. Despite that, efforts are likely to continue as law enforcement officials such as former AG Barr continue to warn about how encryption "in warrant-proof form jeopardizes public safety" and is a net negative to security (Barr, 2019a).

The Open Access Movement

A popular monetization method for academic publishers is to charge readers for access to journals or articles; in a way, this is a form of data hiding. Open access advocates argue that traditional monetization stifles innovation and public good by limiting access to research. They seek alternative monetization and publishing schemes.

The Budapest Open Access Initiative maintains that "By 'open access'" to peer-reviewed research literature, "we mean its free availability on the public internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of these articles" (2012). Open access (OA) can be roughly divided into two models: gold or green (Fitzgerald & Jiang, 2020; Kieńć, 2015). Gold OA generally refers to when a publisher makes a paper or journal free to access, but this is often at a large expense of an author or their institution; Elsevier, for example, charges up to 5000 USD per article (Elsevier, 2021). Green OA generally refers to self-archiving, where a publisher allows an author to make their paper available through means such as a personal website or institutional repository, with some restrictions but fewer fees.

Academics supporting OA like Tennant et. al made numerous arguments about the benefits of OA (2016). They argue that OA can reduce costs for all involved parties, including researchers, academic institutions, and public funding sources. They also say OA has societal benefits, such as higher equitability (e.g., poorer institutions can benefit from accessing OA research) and higher impact as measured by certain metrics (social media mentions and article citations).

Public funding sources, academic institutions, and other groups have promoted OA publishing. All studies funded by the US NIH must be archived on PubMed, a government funded OA archive, within 12 months of original publication (NIH, 2014). The University of California (UC) issued a policy requiring authors within UC to make their works available in UC's OA repository (UC, 2015).

Some groups illegally distribute paywalled research. The website Sci-Hub was estimated to provide free access to about 85 percent of paywalled research articles (Himmelstein et al., 2018). Analysis of Sci-Hub logs found that the site served 28 million documents in the 6 months

between September 2015 and February 2016. (Bohannon, 2016). Bohannon found that Sci-Hub was used even in wealthy countries, with the US being fifth in Sci-Hub downloads. An American PhD student, Gil Forsyth, was quoted by Bohannon as saying that Sci-Hub "will just work" over using her institution to legally obtain access.

Publishers such as Elsevier have responded to the threat posed by both legal OA and illegal distribution channels. Director Heather Joseph of the Scholarly Publishing and Academic Resources Coalition (SPARC), an OA advocacy, commented that "Elsevier has had some difficulties with the concept of open access becoming the norm" (Peterson, 2013). For example, Peterson found Elsevier supported the Research Works Act which would have overturned the NIH's PubMed OA mandate. Regarding illegal content, Elsevier issued takedown notices to Harvard University and other institutions for articles posted on faculty websites. Elsevier has also issued lawsuits against Sci-Hub, has called it "a malicious site used for nefarious purposes," and has offered advice to institutions for how to block Sci-Hub (Erkal, 2019).

Conclusions

So far, the three issues of Profitable Data, Encryption, and Academic OA have been discussed separately. However, tactics used in each of the three cases have implications in the broader area of data hiding and finding. First, we observe that some groups are already engaged in multiple areas of data hiding/finding activities. The EFF has made comments on consumer privacy law like the CCPA, intervened in the Apple encryption dispute, and has also issued a call to action regarding the Fair Access to Science and Technology Act, a proposed OA bill (Harmon, 2017). Facebook also had its own campaigns regarding profitable data and the Apple encryption dispute, as well as creating open source software projects (Vinnik, 2020). Though the

issue of open source is very different from open access, they do share some principles like the belief that knowledge can be shared for public good.

Second, we note the role of government legislation regarding data hiding/finding. While the US legislators are active in all three areas discussed, no comprehensive action has been taken in any discussed case recently. Federal legislation has mostly been limited to proposals, with the exception of promoting OA for NIH-funded studies. Some states have passed substantial consumer privacy bills, but many have not; encryption legislation is also lacking. State OA backing is mostly by state academic institutions rather than through legislation. This lack of legislation is often in spite of executive branch advocacy, as in the case of law enforcement and encryption.

Third, an organization can be both a data hider *and* a data finder in different contexts. Facebook is a data finder in the case of its ad revenue business model, but a data hider advocating for encryption for security purposes. Law enforcement and other executive agencies routinely use encryption to secure their own data.

Fourth, individual action can exert substantial pressure but does not always. For example, Sci-Hub is used by unorganized individuals, but its existence has been enough to cause Elsevier to file costly lawsuits and publish press releases against it. In contrast, individuals have had limited success in altering the policies of businesses that profit off of consumer data. The most substantial changes affecting Facebook are Apple's technology changes and laws like the CCPA rather than individual boycotts.

Future Work

This work visits three areas of data hiding/finding, but even in those areas more can be explored. In-depth examination of end-to-end encrypted messaging, OA/OA hybrid journals, and the role of donations to political campaigns are just a few examples. Broader areas that could be explored include patent law and intellectual property sharing, open source software licensing, the open data movement, and more. Examining areas such as these and with a scope outside of the US could result in more and deeper findings.

References

Aas, J., & Gran, S. (2020, February 27). Let's Encrypt has issued a billion certificates. https://letsencrypt.org/2020/02/27/one-billion-certs.html

Apple. (2021a). Privacy—Features. Apple. https://www.apple.com/privacy/features/

Apple. (2021b). User privacy and data use. Apple Developer. https://developer.apple.com/app-store/user-privacy-and-data-use/

Apple. (2021c). A day in the life of your data: A father-daughter day at the playground. https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and privacy: Concerned confused and feeling lack of control over their personal information. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Barr, W. (2019a, July 23). Attorney General William P. Barr delivers keynote address at the International Conference on Cyber Security. https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber

Barr, W. (2019b, October 4). Attorney General William P. Barr delivers remarks at the Lawful Access Summit. https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit

BIS. (2017, August 15). Encryption and Export Administration Regulations (EAR). Bureau of Industry and Security. https://www.bis.doc.gov/index.php/policy-guidance/encryption

Blankstein, A. (2016, February 16). Judge forces Apple to help unlock terror shooter's iPhone. NBC News. https://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701

Bohannon, J. (2016, April 25). Who's downloading pirated papers? Everyone. *Science*. https://www.sciencemag.org/news/2016/04/whos-downloading-pirated-papers-everyone

Butler, A., Rotenberg, M., & Thomson, A. (2016). Brief of amicus curiae Electronic Privacy Information Center (EPIC) and eight consumer privacy organizations. https://epic.org/amicus/crypto/apple/EPIC-Amicus-Brief.pdf

Buttar, S. (2016, February 20). Apple, Americans, and Security vs. FBI. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2016/02/apple-americans-and-security-vs-fbi

California OAG. (2018, October 15). California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

CBS News. (2016, March 18). CBS News poll: Americans split on unlocking San Bernardino shooter's iPhone. https://www.cbsnews.com/news/cbs-news-poll-americans-split-on-unlocking-san-bernardino-shooters-iphone/

Commerce (2020). U.S. Department of Commerce. Quarterly retail e-commerce sales. https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Congressional Record. (2019, September 25). H.R.4170 - 116th Congress (2019-2020): ENCRYPT Act of 2019 (2019/2020). https://www.congress.gov/bill/116th-congress/house-bill/4170

Congressional Record. (2020a, June 23). S.4051 - 116th Congress (2019-2020): Lawful Access to Encrypted Data Act (2019/2020). https://www.congress.gov/bill/116th-congress/senate-bill/4051

Congressional Record. (2020b, July 30). H.R.7891 - 116th Congress (2019-2020): Lawful Access to Encrypted Data Act (2019/2020). https://www.congress.gov/bill/116th-congress/house-bill/7891

Cook, T. (2016, February 16). Customer letter. Apple. http://www.apple.com/customer-letter/

Cornu, D. (2016, February 2). All Shopify stores now use SSL encryption everywhere. Shopify. https://www.shopify.com/blog/73511365-all-shopify-stores-now-use-ssl-encryption-everywhere

Crocker, C. C. and A. (2019, August 27). U.S. Export Controls and "Published" Encryption Source Code Explained. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2019/08/us-export-controls-and-published-encryption-source-code-explained

Deckelmann, S. (2020, February 25). Firefox continues push to bring DNS over HTTPS by default for US users. The Mozilla Blog. https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users

Decker, E., Donahue, P., & Wilkison, T. (2016). Government's reply in support of motion to compel and opposition to Apple Inc.'s motion to vacate order. US Department of Justice. https://www.justice.gov/usao-cdca/file/832166/download

Elsevier. (2021, March 8). What does it cost to publish gold open access? Elsevier Journal Article Publishing Support Center. https://service.elsevier.com/app/answers/detail/a_id/5972/supporthub/publishing/~/what-does-it-cost-to-publish-gold-open-access%3F/

Erkal, E. (2019, December 20). Allegations linking Sci-Hub with Russian intelligence. Elsevier Connect. https://www.elsevier.com/connect/allegations-linking-sci-hub-with-russian-intelligence

Facebook. (2020a, January 29). Facebook reports fourth quarter and full year 2019 results. https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx

Facebook. (2020b, December 16). Speaking up for small businesses. Facebook for Business. https://www.facebook.com/business/news/ios-14-apple-privacy-update-impacts-small-business-ads

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, *55*, 102181. https://doi.org/10.1016/j.ijinfomgt.2020.102181

Finkle, J. (2016, February 24). Solid support for Apple in iPhone encryption fight: Poll. *Reuters*. https://www.reuters.com/article/us-apple-encryption-poll-idUSKCN0VX159

Fitzgerald, S. R., & Jiang, Z. (2020). Scholarly publishing at a crossroads: Scholarly perspectives on open access. *Innovative Higher Education*, *45*(6), 457–469. https://doi.org/10.1007/s10755-020-09508-8

Gaffney, J. (2020). Watching the watchers: A comparison of privacy bills in the 116th Congress. Congressional Research Service. https://crsreports.congress.gov/product/pdf/LSB/LSB10441

Goodin, D. (2021, January 6). WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app. Ars Technica. https://arstechnica.com/tech-policy/2021/01/whatsapp-users-must-share-their-data-with-facebook-or-stop-using-the-app/

Google. (2021). HTTPS encryption on the web. Google Transparency Report. https://transparencyreport.google.com/https/overview?hl=en

Graham, M. (2020, December 16). Facebook blasts Apple in new ads over iPhone privacy change. CNBC. https://www.cnbc.com/2020/12/16/facebook-blasts-apple-in-new-ads-over-iphone-privacy-change-.html

Greene, D., Cohn, C., Tien, L., Opsahl, K., Lynch, J., Cardozo, N., Cope, S., Crocker, A., & Williams, J. (2016). Brief of amici curiae Electronic Frontier Foundation and 46 technologists, researchers, and cryptographers. https://www.eff.org/files/2016/03/03/16cm10sp_eff_apple_v_fbi_amicus_court_stamped.pdf

Harmon, E. (2017, August 11). Open access can't wait. Pass FASTR now. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2017/08/open-access-cant-wait-pass-fastr-now

Higgins, D. S., Emily Glazer and Tim. (2021, February 13). Facebook meets Apple in clash of the tech titans—'We need to inflict pain.' *Wall Street Journal*. https://www.wsj.com/articles/facebook-meets-apple-in-clash-of-the-tech-titanswe-need-to-inflict-pain-11613192406

Himmelstein, D. S., Romero, A. R., Levernier, J. G., Munro, T. A., McLaughlin, S. R., Greshake Tzovaras, B., & Greene, C. S. (2018). Sci-Hub provides access to nearly all scholarly literature. *ELife*, *7*, e32822. PubMed. https://doi.org/10.7554/eLife.32822

Iachello, G., & Abowd, G. D. (2005). Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '05*, 91. https://doi.org/10.1145/1054972.1054986

Kieńć, W. (2015, June 3). Green OA vs. Gold OA. Which one to choose? Open Science. https://openscience.com/green-oa-vs-gold-oa-which-one-to-choose/

Kirkham, R., & Greenhalgh, C. (2015). Social access vs. privacy in wearable computing: A case study of autism. *IEEE Pervasive Computing*, *14*(1), 26–33. https://doi.org/10.1109/MPRV.2015.14

Maddigan, M., & Katyal, N. (2016). Brief of amici curiae Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo in support of Apple, Inc. https://cdn3.vox-cdn.com/uploads/chorus_asset/file/6141865/appleBriefasfiled__1___1_.0.pdf

Nierenberg, A. (2020, June 12). Signal downloads are way up since the protests began. *New York Times.* https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html

NIH. (2014, March 25). Frequently asked questions about the NIH public access policy. National Institutes of Health. https://publicaccess.nih.gov/faq.htm

Office of Ann Wagner. (2020, July 30). Wagner introduces bill to protect victims of crime, reject dangerous warrant-proof encryption. https://wagner.house.gov/media-center/press-releases/wagner-introduces-bill-to-protect-victims-of-crime-reject-dangerous

PBS News Hour. (2016, February 17). Judge's order to Apple over attacker phone encryption unlocks privacy concerns. https://www.pbs.org/newshour/show/judges-order-to-apple-over-attacker-phone-encryption-unlocks-privacy-concerns

Peterson, A. (2013, December 19). How one publisher is stopping academics from sharing their research. *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2013/12/19/how-one-publisher-is-stopping-academics-from-sharing-their-research/

Pew Research Center. (2016, February 22). More support for Justice Department than for Apple in dispute over unlocking iPhone. *Pew Research Center - U.S. Politics & Policy*. https://www.pewresearch.org/politics/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/

Reinsel, D., Gantz, J., & Rydning, J. (2018). The digitization of the world from edge to core. International Data Corporation. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

RGS Coalition. (2020, June 25). RGS opposes Lawful Access to Encrypted Data Act. Reform Government Surveillance. https://www.reformgovernmentsurveillance.com/rgs-statement-on-lawful-access-to-encrypted-data-act/

Roth, J., Ring, R., Blavin, J., Patashnik, J., & Green, A. (2016, March 3). Brief of amici curiae Airbnb, Inc.; Atlassian Pty. Ltd.; Automattic Inc.; Cloudflare, Inc.; Ebay Inc.; GitHub, Inc.; Kickstarter, PBC; LinkedIn Corporation; Mapbox Inc.; A Medium Corporation; Meetup, Inc.; Reddit, Inc.; Square, Inc.; SquareSpace, Inc.; Twilio Inc.; Twitter, Inc.; and Wickr Inc. Scribd. https://www.scribd.com/doc/302014025/Apple-Brief-Of-Twitter-And-Other-Web-Companies

Selyukh, A. (2016, March 28). The FBI has successfully unlocked the iPhone without Apple's help. NPR. https://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help

Senate Judiciary Committee. (2020, June 23). Graham, Cotton, Blackburn introduce balanced solution to bolster national security, end use of warrant-proof encryption that shields criminal activity. https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity

Signal. (2021, January 7). Signal team regarding verification delays [Tweet]. *@signalapp*. https://twitter.com/signalapp/status/1347240006444675072

Statt, N. (2021, February 1). Facebook prompt will encourage ad tracking opt-in ahead of Apple's privacy push. The Verge. https://www.theverge.com/2021/2/1/22260274/facebook-prompt-apple-ios-ad-tracking-opt-in-permission-privacy-update

Tankovska, H. (2021, January 27). Facebook users in U.S. Statista. https://www.statista.com/statistics/408971/number-of-us-facebook-users/

Tennant, J., Waldner, F., Jacques, D., Masuzzo, P., Collister, L., & Hartgerink, C. (2016). The academic, economic and societal impacts of Open Access: An evidence-based review [version 3; peer review: 4 approved, 1 approved with reservations]. *F1000Research*, *5*(632). https://doi.org/10.12688/f1000research.8460.3

New York Times. (2016, December 14). Tips. *New York Times.* https://www.nytimes.com/tips

Tsukayama, H. (2021, February 12). Virginians deserve better than this empty privacy law. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2021/02/virginians-deserve-better-empty-privacy-law

UC. (2015, October 23). UC Presidential Open Access Policy. University of California - Office of Scholarly Communication. https://osc.universityofcalifornia.edu/scholarly-publishing/uc-open-access-policies-background/presidential/

Van Alstyne, M. W., & Lenart, A. (2020). Using data and respecting users. *Communications of the ACM*, *63*(11), 28–30. https://doi.org/10.1145/3423998

Vinnik, D. (2020, January 13). Facebook open source year in review: A look back at 2019. Facebook Engineering. https://engineering.fb.com/2020/01/13/open-source/open-source-2019/

Virginia LIS. (2021a). HB 2307 Consumer Data Protection Act. Virginia Legislative Information System. https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+HB2307

Virginia LIS. (2021b). SB 1392 Consumer Data Protection Act. Virginia Legislative Information System. https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392

White, J. B. (2016, April 13). California phone decryption bill defeated. *The Sacramento Bee*. https://www.sacbee.com/news/politics-government/capitol-alert/article71446037.html

Whitehead, M. (2020, January 8). Why people leave Facebook – and what it tells us about the future of social media. The Conversation. http://theconversation.com/why-people-leave-facebook-and-what-it-tells-us-about-the-future-of-social-media-128952

Zakrzewski, C. (2021, March 2). Virginia governor signs nation's second state consumer privacy bill. *Washington Post*. https://www.washingtonpost.com/technology/2021/03/02/privacy-tech-data-virgina/