Balkanizing Social Media

IDO KILOVATY*

Ever since the internet has become a truly global phenomenon, for better or worse, there have been debates over whether the global internet needs to be fragmented into smaller, nationalized pieces.[1] This has been true in authoritarian regimes like Russia[2] and China,[3] inching towards heavily monitored and filtered internets, separate from the global internet that we have all gotten accustomed to.[4] The same debates have also been taking place in democratic regimes in the wake of the Snowden revelations,[5] as the growing distrust in the U.S.-controlled internet has led these countries to consider the creation of their own domestic internet.

Enter David Sloss's *Tyrants on Twitter*,[6] a book that thoroughly diagnoses the problem of information warfare conducted on U.S.-based social media platforms by China and Russia. According to Sloss, calling it information *warfare* denotes the seriousness of the phenomenon and how it threatens,

* Frederic Dorwart and Zedalis Family Fund Associate Professor of Law, University of Tulsa College of Law.

[1] Mark A. Lemley, *The Splinternet*, 70 DUKE L.J. 1397, 1400 (2021) (arguing that the Internet is being balkanized); James Ball, *Russia Is Risking the Creation of a "Splinternet"—And It Could Be Irreversible*, MIT TECH. REV. (Mar. 17, 2022), https://perma.cc/FA64-AJA4 ("[I]instead of the single global internet we have today, we have a number of national or regional networks that don't speak to one another and perhaps even operate using incompatible technologies.").

[2] Ball, *supra* note 1.

[3] Geremie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED (June 1, 1997, 12:00 PM), https://perma.cc/XC94-MXHW; Noah Smith, *Balkanization Is Bad for Facebook's Business*, BLOOMBERG (July 3, 2020, 7:00 AM EDT), https://perma.cc/DAX7-P54Z.

[4] Smith, *supra* note 3.

[5] *See generally* Matthew Taylor et al., *NSA Surveillance May Cause Breakup of Internet, Warn Experts*, THE GUARDIAN (Nov. 1, 2013, 12:03 EDT), https://perma.cc/FHU8-YQFH; Jonathan Watts, *Brazil to Legislate on Online Civil Rights Following Snowden Revelations,* THE GUARDIAN (Nov. 1, 2013, 12:16 EDT), https://perma.cc/M67Z-GY5U.

[6] *See generally* DAVID L. SLOSS, TYRANTS ON TWITTER: PROTECTING DEMOCRACIES FROM INFORMATION WARFARE (2022).

and potentially erodes, liberal democracies in the world.[7] Indeed, the problem of information warfare is well-documented, and its destructive nature is generally undisputed.[8] For example, in the last few years, U.S. social media platforms themselves have employed moderators whose role is to investigate, monitor, and suspend accounts linked to foreign regimes and engaged in information warfare.[9] Despite those efforts, information warfare has been permeating social media platforms in recent years.

To tackle the problem of Russian and Chinese information warfare on social media platforms, Sloss proposes a regime of nationality verification for any public user on U.S. social media.[10] According to this proposal, users on social media will have to verify their nationality with their home government, which in turn will greenlight the user's registration and participation on the social media platform. To achieve this, Sloss calls for the creation of the "Alliance for Democracy," a group of democratic nations whose citizens will be allowed to have public accounts on social media. If the registration system is implemented, foreign agents residing outside of the Alliance for Democracy, such as those in Russia or China, will not be allowed to participate on U.S. social media platforms.

Sloss is fully aware of the challenges with such verification systems, in particular the many data security and privacy ones.[11] For example, Chinese and Russian agents may be able to hack public social media accounts, purchase hacked accounts on the dark web, or pay a legitimate user in order for them to engage in information warfare.[12] The same foreign agents would also be able to circumvent the verification system by using compromised credentials, such as U.S. passport photos and social security numbers, to create seemingly legitimate accounts on U.S. social media.[13] While these are serious concerns, they could be addressed at the outset of the verification system's design. In other words, if the system is designed properly, Sloss says, these weaknesses will be resolved. Some examples include features like encryption, hashing, data retention, and more. All in all, even Sloss admits that the verification system is not foolproof, as excluded states would still try to penetrate the digital gate imposed by the registration system. Yet, despite these inherent flaws in such a system, Sloss's proposal is not to eliminate information warfare entirely, but rather to increase the costs of

---

[7] *Id.* at 4.

[8] *See* Waseem Ahmad Qureshi, *Information Warfare, International Law, and the Changing Battlefield*, 43 FORDHAM INT'L L.J. 901, 914–19 (2020).

[9] *See, e.g.*, Twitter Safety, *Disclosing Networks of State-Linked Information Operations*, TWITTER (Feb. 23, 2021), https://perma.cc/58WH-PBUS (disclosing an information warfare network of Twitter accounts which were removed by Twitter).

[10] SLOSS, *supra* note 6, at 16–17.

[11] *See, e.g.*, SLOSS, *supra* note 6, at 175–77, 209–15.

[12] SLOSS, *supra* note 6, at 147–51.

[13] SLOSS, *supra* note 6, at 147–51.

information warfare on social media to such levels that it becomes less likely (though not impossible) for China and Russia to engage in it on U.S. social media platforms.

This contribution focuses on the data security risks associated with the proposed verification system. At the outset, it is important to note that Sloss does not shy away from these risks, and he provides many observations and prescriptions to these risks.[14] In fact, the proposal itself includes a requirement of "[r]igorous safeguards to protect informational privacy and data security."[15] Indeed, the centralized collection of user data for citizenship verification purposes may serve as an appealing target for authoritarian regimes attempting to bust through the digital gate of U.S. social media. The same registration system would also be appealing from a data standpoint, as these regimes would benefit from accessing, and potentially misusing the registration system data. In other words, data security is even more important given the sensitive nature of the data collected as well as the potential consequences of the data getting compromised by authoritarian regimes. Any compromise to the registration system's data could seriously jeopardize national security, privacy, and the wellbeing of social media users. This essay builds on the data security risks laid out in *Tyrants on Twitter*, and presents them as distinct issues, providing a reflection on each one by making the appropriate recommendations to alleviate them.

I. Basic Cybersecurity and Cybersecurity as a Process

Centralizing the nationality verification process in a government entity would inevitably create distrust among some social media users in the government's capacity to sufficiently safeguard the security of user data pertaining to nationality. Already today, as many as 74% of Americans distrust government institutions in keeping their personal data private and secure.[16] The distrust is understandable when one considers the many data breaches that afflicted the U.S. government in recent years. For example, the 2015 Office of Personnel Management (OPM) breach compromised the "sensitive information, including the Social Security numbers (SSNs) of 21.5 million individuals" which included "19.7 million individuals that applied for a background investigation."[17] The question then is, how should the government safeguard the data collected by the verification system to minimize the distrust that some users may experience? To deal with the distrust, one must ask what its causes are. In this context, there may be many

---

[14] SLOSS, *supra* note 6, at 175–77.

[15] SLOSS, *supra* note 6, at 146.

[16] *Most U.S. Citizens Want Government Agencies to Strengthen Cyber Defense Mechanisms to Protect Their Digital Data, Accenture Research Finds*, ACCENTURE (Apr. 10, 2017), https://perma.cc/WYM6-22SY.

[17] *Cybersecurity Incidents*, U.S. OFF. OF PERS. MGMT., https://perma.cc/6MRU-RBY9 (last visited Nov. 24, 2022).

potential responses.

First and foremost, one should assume that many of the data breaches seen in recent years were entirely preventable.[18] While not offering silver bullet solutions, the knowledge and experience developed over the years by information security specialists offer some basic security practices that significantly reduce the likelihood of a data breach, as well as the fallout in case of a breach. The OPM breach is a good example of the unfortunate consequences of the failure to instate basic security features like two-factor authentication.[19] A security audit by the OPM Inspector General determined that the OPM failed to secure its sensitive data, among other things, because its information security was managed by unqualified, uncertified personnel.[20]

While the OPM has since improved its cybersecurity practices, the Government Accountability Office has reported that further security implementations are required.[21] For example, the OPM did not implement its own security policies in all of its assets. Technically, this means that some sensitive data was not encrypted when it should have been.[22]

The two key takeaways from the 2015 OPM breach are as follows. First, implementing basic cybersecurity practices is the single most important step in securing sensitive data. Second, cybersecurity is a process rather than a list of checkboxes. There is a constant need to reevaluate the organization's cybersecurity posture and implement new policies and safeguards to keep up with hacking trends.

For the registration system proposed by Sloss, the lesson would be the same. Indeed, implementing rigorous security measures is important, but the cybersecurity of the system would have to be reevaluated periodically to ensure that it is not breached.

II. Data Retention

With the basic cybersecurity in mind, another important issue is data retention. Assuming that the data is secure against external hackers, how long should the government keep the data collected through its user registration system? As Sloss points out, the government would be expected

---

[18] *See* Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), https://perma.cc/F9U8-868R ("The OTA's analysis of security breaches . . . 'found that 93% were avoidable . . . .'"); Zack Whittaker, *Equifax Breach Was 'Entirely Preventable' Had It Used Basic Security Measures, Says House Report*, TECHCRUNCH (Dec. 10, 2018, 4:20 PM EST), https://perma.cc/DU84-JM2M.

[19] Thu T. Pham, *OPM Security Audit: No Two-Factor Authentication*, DUO SEC. (June 10, 2015), https://perma.cc/3P8G-U5P2.

[20] *Id.*

[21] OPM Has Improved Controls, but Further Efforts Are Needed, No. GAO-17-614 10 (GAO 2017), https://perma.cc/PW5S-PF54.

[22] *Id.* at 18–19.

"to destroy records obtained during the account registration process after a relatively brief time period."[23] However, there is currently no mandatory U.S. law on data retention.[24] If anything, it is likely that the U.S. government would want to keep some of the data collected by the verification system, especially in cases of suspicious online activity by certain users. But the U.S. government's hunger for personal data is not without criticism, and in recent years, there have been calls for Congress to enact privacy and cybersecurity statutes to address issues such as data retention, remedies, and mandatory safeguards.[25] Some of these calls have been inspired by the General Data Protection Regulation (GDPR), which requires that the data collector keep the personal data for "no longer than is necessary for the purposes for which the personal data are processed."[26]

Due to the centralized nature of the user registration process, any government entity holding user information in its database may be an appealing target for data breaches, especially by authoritarian regimes. India's Aadhaar, the largest biometric ID database in the world, has been subject to multiple breaches, exposing the personal data of more than 1 billion people, which are now reportedly on sale on apps like WhatsApp for as little as ten dollars.[27] The same fate could threaten the user registration system if data retention is not taken seriously.

While data retention is one of the most critical data security issues, it is not by any means the only one. Storing user information for only a brief, not-more-than-necessary period of time is essential, but inevitably, some information will be nonetheless stored in the centralized database. It is therefore just as important, if not more, to secure the information that exists at any single point in time in the database. Encryption may offer one tool to address the risk faced by such information. Access controls would similarly limit the access to the information on a need-to-know basis. All in all, the user registration database should not store sensitive information for longer than is necessary.

III. Encryption and Hashing

As Sloss aptly notes, "both companies and government entities" would

---

[23] SLOSS, *supra* note 6, at 176.

[24] *See Mandatory Data Retention*, ELEC. FRONTIER FOUND., https://perma.cc/QP7J-3YDM (last visited Nov. 24, 2022).

[25] *See* Jacob Bogage & Cristiano Lima, *House and Senate Members Unveil Stalled Data Privacy Bill*, WASH. POST, https://perma.cc/4K49-RDP4 (last updated June 3, 2022, 3:00 PM EDT).

[26] Official Journal of the European Union, 'Article 5, Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' OJ L 119 1-88 (Apr. 5, 2016), https://perma.cc/V4KF-ZQ4U.

[27] Ashish Malhotra, *The World's Largest Biometric ID System Keeps Getting Hacked*, VICE (Jan. 8, 2018, 11:07 AM), https://perma.cc/74KX-EJ2Z.

have to use hashing to store account registration information securely. Hashing, Sloss explains, is "a special cryptographic function to transform one set of data into another of fixed length by using a mathematical process."[28] Indeed, hashing is an important data security practice to ensure that any compromise would not reveal to the adversary the plaintext of the stored data.

Encryption is a powerful and vital tool to securely store account registration information as securely as possible. In other words, even if a compromise of data is successful by either China or Russia, the attackers would not have access to the actual information, which could otherwise allow foreign agents to register imposter accounts on U.S. social media platforms.[29]

In addition, strong encryption is essential for the effective protection against attempts to hack or interfere with the functioning of the user registration system. One example of encryption technology that would be desirable in this context includes digital signatures, to provide for secure "authentication, integrity, non-repudiation, and privacy/confidentiality" of the database.[30]

In the context of both Russia and China, the need for strong encryption of user registration information is even stronger. The race for quantum computing technology among the superpowers means that encryption protocols commonly used today may not be secure once quantum computing is achieved. To this end, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has recently announced the selection of four quantum-resistant encryption algorithms that would ensure data security even in the wake of quantum computers,[31] which both China and Russia are racing to attain.[32]

IV. Government Access to User Registration Information

As *Tyrants on Twitter* proposes, we need "bright-line limits on the government's authority to retain and utilize data disclosed to the government under the social media registration system."[33] Such a bright-line limit or rule would have to establish the access control aspect of data security, meaning who can access the data, as well as under what circumstances the data may be accessed. While such a rule is much needed

---

[28] SLOSS, *supra* note 6, at 176.

[29] SLOSS, *supra* note 6, at 147.

[30] SANS INST., INFORMATION WARFARE: CYBER WARFARE IS THE FUTURE WARFARE 12 (2004), https://perma.cc/3M3Q-RCGR.

[31] *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*, NAT'L INST. OF STANDARDS & TECH. (July 5, 2022), https://perma.cc/S2BK-LBFS.

[32] Zhanna Malekos Smith, *Make Haste Slowly for Quantum*, CTR. FOR STRATEGIC & INT'L STUD. (Feb. 11, 2022), https://perma.cc/ZWW9-QZQB.

[33] SLOSS, *supra* note 6, at 210.

to ensure that data is private and secure, save for the narrowly defined exceptions, it needs to clearly establish the penalties should the rule be broken.

Establishing penalties for access to data in violation of the government's data access policy would be needed to address the insider threat problem, which the Cybersecurity & Infrastructure Security Agency (CISA) defines as "the potential for an insider to use their authorized access . . . to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities."[34] In particular, such limits and penalties are much needed in a post-*Van Buren v. U.S.* world, where computer crime laws do not apply to insiders using their authorized access to information for "bad" purposes.[35] One such example is the many instances in which National Security Agency (NSA) employees used surveillance information to spy on their lovers.[36] Therefore, the user registration information database would have to be on a need-to-know basis,[37] and even then, with clear penalties for any violations of the data access policies, which should be clearly delineated.

V. Ensuring Public-Private Cybersecurity

Due to the nature of the user registration system, its design would likely have to focus on information sharing, a data pipeline of sorts, between the government (the verifier) and the social media platforms. It is likely to assume that any such system would not necessarily have to be the direct sharing of user registration information (such as passport/ID copies, social security numbers, etc.) between the government and social media platform, as the government would simply be acting as a verifier who can securely "vouch" for a certain user as being the national of an Alliance for Democracy member state by using authentication tokens.[38]

Nonetheless, the newly emerging relationship under the user registration proposal would involve the government and social media. This relationship may seem uneasy to some, especially when private tech companies are co-opted to do the government's bidding. From a similar perspective, the co-optation of U.S. social media platforms to do the government's bidding (e.g. the exclusion of foreign agents from authoritarian regimes from U.S. social media platforms) may encourage the

---

[34] *Defining Insider Threats*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://perma.cc/T8TB-TV2P (last visited Nov. 24, 2022).

[35] *See* Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

[36] Evan Perez, *NSA: Some Used Spying Power to Snoop on Lovers*, CNN, https://perma.cc/6P7U-WTX4 (last updated Sep. 27, 2013, 7:58 PM EDT).

[37] SLOSS, *supra* note 6, at 177.

[38] *See Authentication Token*, FORTINET, https://perma.cc/K8UL-ZTXU (last visited Nov. 24, 2022).

excluded authoritarian regimes to look for alternative methods of destabilization and disruption.

One such alternative attack method would be more disruptive and less verbal than information warfare—attacks against the social media platforms themselves. This could, for example, result in an increase of distributed denial-of-service attacks against U.S. social media platforms. This is considering the fact that U.S. social media platforms will remain part of the global internet, which they likely would. If left unprepared, these attacks may lead to further user distrust in social media platforms, and potentially the global internet as a whole.

All in all, any hindrance on authoritarian regimes' ability to engage in information warfare could result in cyber-attacks elsewhere. It would be wise for both the government and the tech industry to prepare for a world of balkanized social media.

CONCLUSION

Tyrants on Twitter is a bold call for action. It proposes the balkanization of social media to restrict access to foreign agents from non-democratic regimes, and to a certain extent, ordinary citizens from those regimes. The proposal is compelling, though not without issues. Data security and privacy remain major hurdles in this context, some of which are explored in this symposium piece. Further design and refinement of the registration system may resolve some of these issues, though it is unclear whether social media platforms would welcome such a paradigm shift. It remains to be seen whether information warfare efforts will continue to proliferate on social media platforms, or whether social media can deal with the problem on their own. If not, Sloss's proposal may seem reasonable to tackle the dangerous problem of information warfare online.