American University National Security Law Brief

Volume 13 | Issue 2 Article 4

2023

Hanging in the Balance: An Assessment of European Versus American Data Privacy Laws and Threats to U.S. National Security

Dara Paleski

HANGING IN THE BALANCE: *AN ASSESSMENT OF EUROPEAN VERSUS AMERICAN DATA PRIVACY LAWS AND THREATS TO U.S. NATIONAL SECURITY*

DARA PALESKI

Social media has quickly become an integral part of modern-day life, keeping the world connected to friends, family and current events. Social media, and the data collected from it, also play a crucial role in intelligence gathering and the safeguarding of national security. It is estimated that about 80-95% of information that is collected for intelligence missions is found freely throughout the internet or other publicly available sources.[1] This type of information has been dubbed SOCMINT (Social Media Intelligence) and it has become a crucial tool within the intelligence community.[2] After the Edward Snowden leaks in 2013 revealed a global scale surveillance program on U.S. and international citizens, tensions surrounding data privacy ignited.[3] The European Union (EU) responded to privacy concerns by enacting the General Data Privacy Regulation (GDPR).[4] The GDPR has been hailed as one of the "most comprehensive attempts to globally regulate the collection and use of personal data by both governments and the private sector."[5] The GDPR shows that the European Union has taken strides to protect both the privacy of their citizens and their transnational security. The U.S., however, has not been as zealous in their response to citizens' data privacy concerns. Currently, the U.S. still has no comprehensive federal legislation to protect personal data.[6] This has proven to become a national security risk and will continue to threaten the national security landscape until the federal government addresses America's lack of data privacy protections.

---

[1] ETH ZURICH, *CSS Analyses in Security Policy*, (2008), https://www.files.ethz.ch/isn/50169/css_analysen_nr%2032-0408_E.pdf; *See also*, Sofia Charania, *Social Media's Potential in Intelligence Collection*, 33 AM. INTELL. J. 94 (2016).
[2] Social Media Intelligence (SOCMINT) is a form of Open-Source Intelligence (OSINT). *See* Sir David Omand, Jamie Bartlett & Carl Miller, *Introducing Social Media Intelligence (SOCMINT)*, 27:6 Intelligence and National Security 801, 801-823 (Dec. 2012).
[3] Rachel L. Brand, *Balance in Intelligence Gathering and Privacy*, THE HILL (Dec. 15, 2015), https://thehill.com/blogs/congress-blog/homeland-security/263143-balance-intelligencegathering-and-privacy.
[4] Regulation 2016/679, art. 94, 2016 O.J. (L 119).
[5] Human Rights Watch, *The EU General Data Protection Regulation*, HUMAN RIGHTS WATCH (2018), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation.
[6] Daniel Castro & Ashley Johnson, *Why Can't Congress Pass Federal Data Privacy Legislation? Blame California*, itif.org (2019), https://itif.org/publications/2019/12/13/why-cant-congress-pass-federal-data-privacy-legislation-blame-california.

TABLE OF CONTENTS

I. THE SOCIETAL BACKDROP OF EUROPEAN AND AMERICAN PRIVACY LAWS

Prior to modern legislation, European "privacy laws" were housed in Article 8 of the European Convention on Human Rights.[7] The Article provided a right to protect one's "private and family life, his home and his correspondence".[8] The Article has been used to safeguard aspects of personal life and dignity, ranging from LGBTQ+ rights to mental health awareness.[9] The core concept of preserving personal dignity can be exemplified by case law. In *Peck v. United Kingdom*, CCTV footage of a man attempting suicide was published by local authorities without his consent. No sufficient attempts were made to mask his identity.[10] Police could have easily blurred out Mr. Peck's face, but did not do so, and instead broadcast the footage with his face in view. Peck's story became a media sensation, despite his distress and humiliation. Peck subsequently appeared on television broadcasts to explain his actions in order to mitigate the damage to his reputation. Eventually, the European Court of Human Rights held that the distribution of the CCTV footage without Peck's consent was a violation of Art. 8 protections. Though the intrusion of privacy was at the hands of local government officials, the damage to Peck's reputation and dignity was at the forefront of the case's decision.

In the United States, there is a more prominent emphasis on the prevention of government intrusion and protection of freedom of speech, rather than considerations towards reputation. This interpretation dates back to the Revolutionary War and English intrusion upon the private lives of

---

[7] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8.
[8] *Id.*
[9] *Case of Oliari and Others v. Italy*, Applications Nos. 18766/11 & 36030/11 (July 21, 2015) (holding that government interference that prevented gay couples from obtaining civil partnerships violated Art. 8); *Peck v. United Kingdom* (2003) 36 EHRR 41.
[10] *Peck v. United Kingdom* (2003) 36 EHRR 41 (finding that Although the applicant was on a public street, he was not there for the purposes of participating in any public event and could not have foreseen that his walking down the street would be shown to such a wide audience; Mr. Peck's consent could have been obtained prior to the broadcast; His identity could have been masked with the use of technology and Mr. Peck's subsequent media interviews criticizing the use of the CCTV footage did not constitute a desire to be revealed to the public eye.)

early colonial settlers.[11] In the case of *Florida Star v. B.J.F.,* SCOTUS found that there were no violations of privacy rights when a Florida newspaper leaked the name of a rape victim.[12] Here, the Court assessed Florida's interests in protecting the identities of rape victims versus the constitutionally protected freedom of the press to publish truthful, lawfully obtained information. A Florida statute prevented the publishing of rape victims' identities through instruments of "mass communication."[13] B.J.F claimed that her privacy and safety was violated, and if the court allowed the Florida Star to go unpunished, it would prevent future rape victims from coming forward in fear of public exposure. The Florida Star claimed they had a constitutional right to publish the material since they lawfully obtained the truthful information and because violent crimes are a matter of public importance.[14] Ultimately, SCOTUS decided that the First Amendment concerns outweighed the state's interest, holding that "[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[15] Ten years after the *Florida Star* case, SCOTUS handed down decisions in two similar cases in *Wilson v. Layne* and *Hanlon v. Berger*. In both cases the Court held that police officers violated the Fourth Amendment rights of homeowners when they allowed members of the press to accompany them during the execution of a warrant in their homes.[16]

---

[11] The prevention of government intrusion is a core principle of American law which can be seen throughout the Bill of Rights. *See* Daniel J. Solove, A Brief History of Information Privacy Law in PROSKAUER ON PRIVACY, PLI (2006). https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.; *See also*, *Whalen v. Roe*, 429 US 589 (1977) (discussing that Americans will usually see privacy violations whenever the state is involved).

[12] *Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

[13] Fla. Stat. Ann. § 794.03 (1987)

[14] 491 U.S. 524 at 526.

[15] *Id.* at 533.; *See also Sipple v. Chronicle Publishing Co*., 154 Cal. App. 3d 1040, 1043 (holding that a tortious invasion of one's privacy is exempt from liability if the publication of private facts is truthful and newsworthy.)

[16] *Wilson v. Layne*, 526 U.S. 603 (1999) (finding that police officers violated the Fourth Amendment by permitting media ride-alongs, but failed to address if Wilson's privacy was violated); *Hanlon v. Berger,* 526 US 808 (1999) (stating that police violate the Fourth Amendment rights of homeowners when they allow members of the media to accompany them during the execution of a warrant in their home).

II. CURRENT PRIVACY FRAMEWORKS

A. The European Union

In 2018, the EU enacted the General Data Protection Regulation (GDPR). The GDPR harmonizes data privacy laws throughout the EU member states. Every EU citizen is protected and every business targeting the EU market is affected. This means that companies who profit off of the EU market must adhere to and comply with GDPR regulations or face penalties for noncompliance, which can amount to 4% of annual global turnover or 20 million Euros, whichever is greater.[17] EU citizens are granted certain protected rights under the GDPR. *The right to be informed* about the collection and usage of their personal data. *The right to access* the data collected on them. *The right to rectify* false or inaccurate information, which must be done without undue delay by the authority collecting data. *The right to be forgotten*, which allows an EU citizen to request that their personal data be deleted. *The right to restriction and processing* of personal data. *The right to data portability*, meaning the right to prevent or allow the transfer of personal data across various services. *The right to object* or to withdraw consent from data processing.[18]

Article 23 of the GDPR houses a "national security exception" to the regulations. Article 23(1)(a) provides that data collectors can disregard the right to be forgotten on the grounds of national security, defense, and public security. The inclusion of the national security exception, though not perfect, shows a desire to promote the protection of EU citizen's data privacy and national security of its member states.

---

[17] GDPR.EU, *FAQ - GDPR*, GDPR.EU (2019), https://gdpr.eu/faq/.
[18] Rohit Thakral, *8 Rights given to every EU citizen by GDPR*, TARGET INTEGRATION (Apr. 18, 2018), https://targetintegration.com/8-rights-by-gdpr-to-eu-citizen/.

In the three years that the GDPR has been in force, it is fair to say that the regulation has been successful in altering the privacy landscape. Since 2021, data protection authorities in the EU have imposed $1.25 billion in fines for breaches of the GDPR.[19] Daily breach notifications to regulators from EU firms is also on the rise, averaging at about 356 per day.[20] Countries and companies have been falling in line to comply with the GDPR as well. Australia, Japan, South Korea, Brazil, and China modelled their privacy legislation on the GDPR.[21] H&M, a clothing retailer, was found to have been collecting and monitoring personal data about their employees without consent. H&M paid the GDPR fine and subsequently adopted remedial measures to implement better data protection policies and compensate those employees affected by the improper data collection.[22] The GDPR has shown that it is possible to protect the rights of the individual while also safeguarding data and national security.

B. The United States

As previously mentioned, the United States has no comprehensive federal data privacy law. Instead, "data privacy" is scattered throughout certain federal laws. Some key examples include HIPAA, GLBA, ECPA, FTCA and COPPA. The Health Insurance Portability and Accountability Act (HIPAA) was created to protect communications between patients and health providers. The Gramm-Leach-Billey Act (GLBA) was enacted in order to protect the personal consumer information stored in financial institutions. The Electronic Communications Privacy Act (ECPA) limits the

---

[19] Ross McKean et al., *DLA Piper GDPR Fines and Data Breach Survey: January 2023 | DLA Piper*, WWW.DLAPIPER.COM (2023), https://www.dlapiper.com/en-au/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023 .

[20] *Id.*

[21] Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, WWW.CSIS.ORG (2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement.

[22] *Id.* "There are many other examples where GDPR fines have led to positive changes in company policies. According to one GDPR tracker, around 100 fines were issued, alongside corrective measures, because of "insufficient technical and organizational measures to ensure information security." By comparison, the total number of fines for not sufficiently fulfilling the data breach notification obligation is only around 20, with the highest fine imposed on Booking.com B.V. for €475,000. That said, the number of breach notifications per day has increased compared to last year." *Id.*