PRIVACY INTERNATIONAL

Submission to Department of Homeland Security, Privacy Office (USA), Regarding DHS Social Media Retention Policy

19 October 2017

Notice of Modified Privacy Act System of Records[1]

Agency: Department of Homeland Security, Privacy Office
Action: Notice of Modified Privacy Act System of Records
Comments Close: 18.10.2017
Document Citation: 82 FR 43556
Agency / Docket Number: DHS-2017-0038
Document Number: 2017 – 19365

Submission via Federal e-Rulemaking Portal

Introduction

Privacy International wishes to raise serious concerns regarding the proposal to expand immigration records to include social media handles, associated identifiable information and search results. Specifically, in relation to the current request for comments[2] Docket Number DHS 2017 0038, we object to the Department for Homeland Security proposal to update record source categories to include "publicly available information obtained from the internet", "commercial data providers" and from "information shared obtained and disclosed pursuant to information sharing agreements".

The Department of Homeland Security's ("DHS") desire to expand the use of *social media intelligence* and *open source intelligence* without sufficient justification that this is necessary and proportionate represents a gross intrusion into the individual's right to privacy.

It restrains autonomy and liberty: it will cause both immigrants and citizens in the US, together with the millions who interact online, to mistrust social media and cause unease in relation to their online activities. This will chill free speech of all internet users who will become concerned to express personal or political views in case such rules could someday apply to them.

For a number of years, DHS has been collecting and scrutinizing the social media of certain immigrants and foreign visitors. The policy applies to a large number of individuals including lawful permanent residents and naturalised U.S. citizens. It would also affect everyone who communicates with those who fall under the regime.

Now that it is clear that DHS sees this as an expandable area for data collection and scrutiny of people's activities, we call for an urgent review of all collection, retention and processing activities not only in relation to this proposal but more broadly of the

[1] https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records

[2] We note that the policy comes into effect the last day comments can be submitted, thus displaying no real intention to consider comments in light of the policy.

use of *social media intelligence* and *open source intelligence* throughout DHS and other government departments.

This form of monitoring is inconsistent with international principles of legality, necessity, and proportionality.

Summary background

DHS proposes to modify the current DHS system of records titled, "Department of Homeland Security / U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection – 001 Alien File, Index, and national File Tracking System of Records" ["A-Files"].

This system of records contains information regarding transactions involving an individual as he or she passes through the U.S. immigration process.[3] A-Files became the official file for all immigration records created or consolidated since April 1, 1944.

However, DHS states that they no longer consider the paper A-File as the sole repository and official record of information related to an individual's official immigration record. An individual's immigration history may be in the following materials and formats: (1) a paper A-File; (2) an electronic record in the Enterprise Document Management System or USCIS Electronic Immigration System; or (3) a combination of paper and electronic records and supporting documentation.

The proposal contains 12 points of expansion on what DHS is allowed to collect. Numbers 5 and 11 are of specific concern to Privacy International, in their ability to reach into the lives of immigrants to the US and anyone who interacts with them, knowingly or unknowingly, without any suspicion of wrongdoing.

From the announcement :

> The Department of Homeland Security, therefore, is updating the "Department of Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection-001 Alien File, Index, and National File Tracking System of Records notice to:
>
> [...]
>
> (5) expand the categories of records to include the following: country of nationality; country of residence; the USCIS Online Account Number; **social**

[3] The purpose of this system of records is to facilitate administration of benefits and enforcement of provisions under the INA and related immigration statuses. A-File (whether paper or electronic), immigration case files, CIS, MiDAS and NFTS are used primarily by DHS employees for immigration processing and adjudication, protection of national security and administering and enforcing immigration and nationality laws and regulated regulations and policy. These records also assist DHS with detecting violations detecting violations of immigration and nationality laws; supporting the referral of such violations for prosecution or other appropriate enforcement action; supporting law enforcement efforts and inspection processes at the U.S. borders; as well as to carry out DHS enforcement, immigration, intelligence and or other homeland security functions.

> **media handles, aliases, associated identifiable information, and search results**; and the Department of Justice (DOJ), Executive Office for Immigration Review and Board of Immigration Appeals proceedings information
>
> [...]
>
> (11) update record source categories to include **publicly available information obtained from the internet**, public records, public institutions, interviewees, **commercial data providers, and information obtained and disclosed pursuant to information sharing agreements**;
>
> [emphasis added]

In addition to the updates noted above, the document states

> *"Alien File, Index, and National File Tracking System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence or other homeland security functions. In addition ... **may be shared with appropriate Federal, State, local, tribal, territorial, foreign or international government agencies** consistent with the routine uses set forth in this system of records notice."*

The term "information sharing agreements" isn't defined in the policy, but it could conceivably cover both the types of surveillance agreements that the US has with countries like the UK, Canada, Australia, and New Zealand in the Five Country Conference (FCC).

Highly invasive

It is through social media that we express our views, our opinions and our sense of belonging to communities. Different generations, communities and individuals have their own context-dependent idiosyncratic way of communicating on social media and interacting online.

To permit the collection of 'social media handles, aliases, associated identifiable information' to enable monitoring of activity on social media platforms and to expand sources to 'publicly available information obtained from the internet' is to give a deep understanding of our social interactions, our habits, our locations, and the pattern of our daily lives. This *social media intelligence* ("SOCMINT") includes monitoring of content, such as messages or images posted, and other data, which is generated when someone uses a social media networking site. The information involves person-to-person, person-to-group, group-to-group and includes interactions that are private and 'public'.

SOCMINT allows for the monitoring of extremely personal data. For example, "Tweets" posted on mobile phones can reveal location data, and their content reveals individual opinions (including political opinions) as well as information about a

person's preferences, sexuality, emotional and health status. This allows a substantial picture to be built of a person's interests, connections, and opinions. Even deeper insight is possible. For instance, in May 2017 Facebook told advertisers it can identify emotions such as teenagers feeling "insecure and worthless".[4]

Wide impact

Social media intelligence does not just affect the person targeted: it affects all the people within their networks. In turn, a review of social media will not be limited to an individual, but extend to friends, relatives, and business associates. It also affects individuals' unknown to the persons targeted if they have been interacting on social media, for example if they are part of the same interest groups on Facebook or respond to the same tweet on Twitter. This is also likely to mean that the social media use of US citizens will be monitored, and in turn chilled, thus impacting their constitutional right to free speech.

There is significant danger of normalising the use of SOCMINT internationally and the resulting reciprocal effects for US citizens applying for visas. For example, when DHS first introduced fingerprinting as part of the US-VISIT programme, Brazil introduced fingerprinting requirements for US citizens, leading to a complaint by US Secretary of State Colin Powell.

By normalising such practices internationally, it undermines the security of US citizens by making their social media activity vulnerable to monitoring by foreign countries' authorities. The world's oppressive regimes have already started on this path. In Thailand for example, the Technology Crime Suppression Division has a 30-person team scanning social media platforms for *lèse-majesté* – speaking ill of the monarchy – allowing them to identify anyone critical of the monarchy, which is punishable by a jail term between 3 and 15 years. British human rights organisation Reprieve reported in 2015 that Saudi Arabia threatened individuals with the death penalty for tweeting and warned that people could face execution for tweeting rumours "which create civil discord, via social media platforms like Twitter." The U.S. is following suit with this form of broad surveillance, quietly endorsing the use of this surveillance, and setting the example for democratic and non-democratic governments alike.

Further, by storing identifiers, it chills the freedom of speech of naturalised citizens who will reasonably fear that their personal data will be exploited in the future for different purposes by different US federal and state agencies.

Automated decision making

Previous proposals and the Officer of Inspector General Report of February 2017 'DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success'[5], indicated that the methods of analysing social media

[4] https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens
[5] https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf

networking sites vary and include manual and automated review. The DHS proposal does not specify what tools will be used.

The February 2017 report noted that agencies have been trialling the use of automated tools including search tools and cross-platform access mechanisms. In relation to the April 2017 pilot the report states:

> *In reviewing the pilot, USCIS concluded that the tool was not a viable option for automated social media screening and that manual review was more effective at identifying accounts. USCIS based its conclusion on the xxxx[6] tool's low "match confidence." Because the resulting accounts identified by the tool did not always match up with the applicants, officers had to manually check the results. However, USCIS did not establish match benchmarks for the tool, so it does not know what level of match confidence would signify success or failure.*

We therefore lack clarity in relation to results of searches and queries of users and activities or types of content users post. The collection of large amounts of personal data for some form of analysis, at the scale proposed, indicates that automated review will be used. We are concerned at the lack of transparency in respect of the use of manual and automated collection techniques and other unspecified 'forms of information technology'.[7] What role do they play in decision making and how can outcomes be challenged?

Automated decision-making, including through the use of profiling, poses significant risks, as we have raised previously with regards to DHS's (withdrawn) Computer Assisted Passenger Pre-screening System (CAPPS II) and the Automated Targeting System.[8] Particularly, since derived, inferred or predicted profiles may be inaccurate, or otherwise systematically biased, profiling may also lead to individuals being misclassified or misjudged. When profiling is used to inform or feed into a decision that affects individuals, the outcome of such decisions may result in harm.

The White House Report 'Big Data: Seizing Opportunities Preserving Values[9]' dated May 2014 noted that profiling was a powerful capacity which allowed the collection and use of information:

> *"to algorithmically profile an individual, possibly without the individual's knowledge or consent."*

The Report warned that:

---

[6] This name is redacted in the report itself

[7] https://www.regulations.gov/document?D=DOS-2017-0032-0001

[8] https://privacyinternational.org/node/361

[9] https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

"A significant finding of this report is that big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education and the marketplace."

"The technologies of automated decision-making are opaque and largely inaccessible to the average person. Yet they are assuming increasing importance … This combination of circumstances and technology raises difficult questions about how to ensure that discriminatory effects resulting form automated decision processes, whether intended or not, can be detected, measured and redressed. We must begin a national conversation on big data, discrimination and civil liberties."

In the words of the UN Human Rights Council:

"automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights"[10]

Unintended consequences and abuse

The collection and processing of social media information may lead unintended consequences and abuse. Given the context specific nature of social media it could lead to misconstrued communications being treated as nefarious and result in rejected visa applications with personal and economic impact. This particularly affects people outside of the U.S. who will have limited rights of redress.

The arbitrary nature of this power, granting officials the ability to deny visas based on their interpretations of an individual's social media history, could result in abuses by individual officers as well as the systematic targeting of certain ethnic and religious group. By way of example, the case of *Raza v. the City of New York* revealed how the New York police were systematically gathering intelligence on the Muslim communities and part of the surveillance involved SOCMINT. It is unclear how there can be guarantees against such abuses given the opaque nature of this power and in view of the lack of supervision and oversight.

Clarification is required

The vague nature of this proposal and lack of elaboration is a serious cause for concern, particularly for all wishing to travel to the US for family, business, diplomatic, and personal reasons. We note a few key unanswered matters:

1. The fifth proposal does not appear to be exhaustive stating the categories of records "include".

[10] **U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)**

2. No definition is provided for “social media handles” / “aliases” / “associated identifiable information” nor whether for example this includes work, personal or other group based social media activity.

3. There is no indication that a list will elaborate on which social media handles, aliases and identifiable information will be targeted.

4. The use of “associated identifiable information” is unacceptably broad and opaque with no clarify in the boundaries for how this can be interpreted.

5. The use of “search results” suggests a worrying desire to use Google or other search engines to look up individuals. It is unclear if the aim is to use Google or other searches such as open source intelligence tools to search the deep web for identifiable information.

6. There is no detail on how this process will operate.

7. No explanation is provided why and how this information is necessary and proportionate to the intended purpose.

8. The source categories appear to bolster the above including “publicly available information obtained from the internet” however no clarify is provided what this will involve and what is meant by “publicly available information”.

9. There is no detail in relation to the use of “commercial data providers” which could include data brokers and third parties who collect and trade in personal data of individuals.

10. Further it refers to “information obtained and disclosed pursuant to information sharing agreements” without elaborating what agreements are being referred to.

11. It was unclear whether the monitoring would take place and when. Would searches be conducted on disclosed social media handles after application process.

12. There is no indication what procedures and safeguards are in place, including safe storage and deletion of data, and effective oversight.

13. There is no indication that individuals will be able to obtain full copies of their files, including electronic sources, to ensure that data held about them is accurate and up to date.

We note the in February 2017**,** the Officer of Inspector General reported on ‘DHS’ Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success’ found that[11]:

[11] https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf

> ‘these pilots, on which DHS plans to base future department-wide use of social media screening, **lack criteria for measuring performance to ensure they meet their objectives.** Although the pilots include some objectives, such as determining the effectiveness of an automated search tool and assessing data collection and dissemination procedures, it is not clear DHS is measuring and evaluating the pilots’ results to determine how well they are performing. Absent measurement criteria, the pilots will be of limited use in planning and implementing an effective, department-wide future social media screening program.’

Procedural issues

We are concerned that the date for comments ends on October 18, 2017, the same day that the modified system will become effective. This allows for no consideration of comments.

The aim to introduce the proposal before considering the comments is a deleterious attitude towards the millions of individuals who interact with social media on a daily basis.

Conclusion

Numerous and important questions remain outstanding and urgently need to be publicly clarified. From the proposal it is clear that here is insufficient justification that this is effective or necessary and proportionate, and as such is an unlawful invasion into privacy.

Social media, which can include a wide range of online platforms and applications, can be revealing and sensitive, making any collection or retention highly invasive. The effect would be unjustified intrusion into the private lives of those affected, undermining their freedom of speech, and affecting everyone in their networks, including US citizens.

By normalising the practice internationally, other state authorities may reciprocate by monitoring the social media of US citizens, undermining their rights as well as their security while travelling.

The potential use of automated decision-making, including through the use of profiling, poses significant risks, since derived, inferred or predicted profiles may be inaccurate, or otherwise systematically biased, leading to individuals being misclassified or misjudged.

Now that it is clear that DHS sees this as an expandable area for data collection and scrutiny of people’s activities, we call for an urgent review of all collection, retention and processing activities not only in relation to this proposal but more broadly of the

use of *social media intelligence* and *open source intelligence* throughout DHS and other government departments.

About Privacy International

Privacy International is a UK-registered charity that promotes the right to privacy at an international level. Established in 1990, Privacy International undertakes research and investigations into state and corporate surveillance with a focus on the technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the US, the United Kingdom and Europe, including the European Court of Human Rights. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy. It also strengthens the capacity of partner organisations in developing countries to do the same.