Abstract
In May 2016, the United States Office of the Director of National Intelligence (ODNI) issued “Security Executive Agent Directive 5” (SEAD-5) (U.S. ODNI, 2016) authorizing the collection, use, and retention of social media information for the personnel security clearance process (PSCP), a process put in place to screen applicants for eligibility for national security and public trust positions. The incorporation of social media was a watershed moment for this process as social media, and even information from the entire Internet, had not been allowed into the investigation process before. The integration was not without resistance to the implementation, though, and backstage concerns about privacy emerged in Congressional hearings. What is most interesting to note, however, is that the resistance was for the most part in support of privacy for the potential employees of whom were receiving the check and the government’s obligations for the information collection; however, there was little, if any, mention of deeper, possibly problematic privacy concerns for the social media platforms and their mediated connections that co-create a second, derivative type of content beyond the access of their users. This paper examines the hearing “Incorporating social media into federal background investigations” in response to the SEAD-5 to see what the U.S. Congress did and did not discuss at the hearing and explores potential explanations for the inclusions/omissions, ultimately answering how those in charge of policies could have overlook deeper privacy complexities, and evaluating what this can mean for government, privacy, and policy researchers.

Contents
1. Introduction
2. Legislation and hearings
3. Methods
4. Resulting Congressional concerns
5. Discussing Congress’ privacy concerns
6. A more macroscopic view
7. Conclusion

1. Introduction
In September 2013, a government contractor with a security clearance named Aaron Alexis brought a sawed-off shotgun into a building at the Washington Navy Yards and killed 12 people before being shot and killed by police. The incident jarred the nerves of both media and government leading to questions of how Alexis, with a reportedly checkered, troubled past full of “red flags,” obtained a clearance to access the secure facility in the first place.
A look at this hearing and Congress’ concerns for the incorporation of social media into the clearance process paints an interesting picture of the role of public policy in regulating technologies, especially those that can disrupt tradition flow of information and potentially jeopardize the privacy of those whose information was collected. When Congress discussed concerns for social media’s inclusion into the process, though, it is of note that they were most often concerned with information privacy and establishing an appropriate flow of information in ways that could be explained through Nissenbaum’s (2011) concept of contextual integrity, or expectations that information will flow in socially anticipated ways. In fact, Congress was essentially involved in establishing the norms for how to handle the information collected. As will be illustrated later, Congress was most interested in cementing authority to gather social media information, wanted to make sure only correct, publicly available information was gleaned, and that information was stored and shared with only authorized parties.

However, while these concerns are a step in the right direction for those that advocate for legislating technologies and privacy, they are also limited. For this particular case, those concerns were largely about user-created content that skims the surface of information that social media sites collect. This is problematic because the objections didn’t go deep enough to mention other forms of privacy from surveillance possibly conducted by the social media platforms. As Mulligan, et al. (2016) summarize, privacy harms can result from not just surface-level content but also deeper, mediated connections such as decisions based on classifications of group data, inferred insights from disclosed content, discovery and collection of personal identifying information, behavior analysis, or de-identified data cross-referencing. But what possible explanations are there for Congress overlooking the deeper content of social media sites? Does this have to be explained through the familiar trope of government ineffectiveness (e.g., Feiner and Graham, 2020; Mullin, 2014; Timmons, 2017)? While it may be easy to criticize an inefficient government or one that privileges technology companies, this paper will ultimately ask, what possible reasons exist for Congress to overlook deeper privacy complexities in their critique of the social media incorporation, and why does this matter? It will then argue there are at least two possible reasons: 1) the complexity of the hearing process; and, 2) the consequences of simplifying the concept of privacy, either due to the hearing constraints or for some other reason. While not the only two possible answers, these conclusions are useful for delving deeper into the process of legislating privacy and offers a generative conversation as to why Congress might have not discussed deeper privacy concerns.

2. Legislation and hearings

To reach these two conclusions, it is first useful to understand the particular genre of which the “Incorporating social media into federal background investigations” is, and examine how Congress legislates technology and privacy. To start out generally, legislation in the United States is often lengthy, complex, and involves the legislative branch of the government which includes both the House of Representatives and Senate. It also involves a range of steps from the introduction of policy, to the debate of processes and legislation, to formalizing policies and procedures (Congress.gov, n.d.).

Congressional hearings are also important parts of the legislative process. Hearings are held for a variety of reasons, such as to get information and opinions about legislation, look at the implementation of federal law, hold investigations into particular areas of interest, evaluate a department’s behavior, or explorations to discuss current pertinent topics (govinfo, n.d.). They are also useful for government transparency because they are civic events where the public can at least watch government proceedings (Hansen, et al., 2011). Hosts of hearings are often committees or subcommittees or a joint combination of the two. Rules around the election of committee members are defined by both
Democrats and Republicans but are limited by Congressional rules of the number of committees where which one can serve as well as the term limits one can spend in the committee.

2.1. Legislating technology

Legislating technologies adds particular complexity to the already complex process because policy makers must continually react to the changing technological landscape [4]. In the U.S., the government debates legislation for a variety of reasons to include how the corporation manages its technology or how the public can also use that technology. For example, for the social media space of YouTube, Gillespie (2010) illustrates that policy-makers had to support the categorization of YouTube as a platform (bringing the semantics of the term with it) and then figure out how to provide space for expressive freedom but also protection from that content’s potential liability. Other ongoing legislative considerations for YouTube range from questions about how YouTube’s services intersect with other laws such as copyright and the Digital Millennium Copyright Act (DMCA) (Hassanabadi, 2011) or the recording of children’s information in conjunction with the Children’s Online Privacy Protection Act (COPPA) (U.S. Federal Trade Commission, 2019).

Committees not only look at how technology companies and the public utilize technologies as in the above example of YouTube, though; Congress is also tasked with assessing the government’s own use of technology. If a government agency wants to incorporate something new, like social media, into their routine procedures, Congress discusses how that can and should be implemented. One committee tasked with institutional reflection is the U.S. House of Representative’s standing Committee on Oversight and Reform (COR). According to the House, this committee is tasked to “review and study on a continuing basis the operation of Government activities at all levels with a view to determining their economy and efficiency.” [5] In the case of this study, two of the COR’s subcommittees, Government Operations and National Security, were the hosts of the hearing.

2.2. Legislating privacy

As will be discussed more in depth later, one particular concern of this hearing was legislating privacy and how incorporating social media could pose privacy concerns for clearance applicants and their associates. Legislating privacy is a more specific area of concern for technological regulation and has been an on-going concern for both the government and scholars, but it is difficult to discuss legislating privacy without at least a basic understanding of privacy. For this paper, a baseline, working description of privacy is that it is a belief, right, process, or legislation with the purpose of controlling visibility for something, be it information, bodies, communications, et. cetera. This definition is loose, however, because privacy itself is contested concept that has been approached in a variety of ways by both policy-makers and scholars. For instance, Koops, et al. (2017) found that in a study of academic legal studies, nine differing constitutions, and legal and philosophical scholarship in those nine countries, privacy is often described in a number of ways, ranging from the controlled visibility of bodies to spaces, communications, proprietary information, intellectual matters, decisions, associations, and behaviors for individuals. Mulligan, et al. (2016) argues that it is not necessarily useful to come up with one definition of privacy but rather to think of it as a contested concept altogether.

One particularly useful way privacy could be framed for this paper and for social media is Nissenbaum’s (2011) notion of “contextual integrity.” Contextual integrity focuses on the flows of personal information in relation to behavioral expectations. As long as an information flow “adheres to entrenched norms,” then the information seems to be kept private [6]. Only after information deviates from expectations does privacy seem jeopardized. For instance, Nissenbaum provides the example of patients’ comforts with doctors having their personal information, but if the doctors then sold that information to marking firms, then one would feel the personal effects of the breach of privacy expectations. For this study, Congress was concerned that information not be shared with particular people that weren’t authorized for access. Again, they were also tasked with determining what the norms for this information should be in the context of the government’s use of the information gleaned from the process.

Contextual integrity is particularly difficult for social media because as Nissenbaum (2011) notes, “Information technologies and digital media have long been viewed as threatening to privacy because they have radically disrupted flows of personal information.” [7] Further, limiting privacies is difficult in itself, but determining limitations online is more complicated “because of shifting recipients, types of information, and constraints under which information flow.” Intersecting audiences in these spaces can range from one’s personal connections, to the public, to the social media platforms and their third-party connections, and the technologies present in these spaces. For instance, as will be discussed later, one Congressman was concerned that one’s loyalty could be called into question if the government sees that one’s familial connections are not from the U.S.
Taking this background of the legislation, technology, and privacy into consideration, it is now useful to begin to answer the main question, how could Congress have overlooked deeper privacy complexities in their critique of the social media incorporation, and why does this matter? To answer this takes three steps. First, it is important to establish that Congress was indeed concerned with privacy, so the paper will answer, (1) how were Congress’ concerns for the incorporation also privacy concerns? This question will be answered through a content analysis of the hearing directly. Second, it is useful to analyze the content of those concerns in a slightly broader assessment to see what could possibly have been overlooked, answering, (2) what do these particular results say about Congress’ conception of privacy? Finally, both responses to those questions help answer the larger research question, (3) how could Congress have overlooked deeper privacy complexities in their critique of the social media incorporation, and why does this matter?

3. Methods

To answer first question of how were Congress’ concerns for the incorporation also privacy concerns, I conducted a content analysis of the House hearing “Incorporating social media into federal background investigations” to identify what Congress was concerned with in the first place, and then further sort those concerns into categories, which ended up with a focus on privacy. The hearing was recorded and transcribed for historical review (U.S. House of Representatives Committee Repository, 2016; C-SPAN, 2016), but the content of the analysis was the written transcription.

To do this study, based on a compilation of various recommendations, I utilized the following six steps. First, in what Elo and Kyngäs’ (2008) might call the preparation phase [8], I selected relevant texts and a unit of analysis as recommended by Mayring (2000). In this case, I chose the SEAD-5 and the resulting Congressional hearing because this document and subsequent discussion reflects a pivotal policy moment for the PSCP in which policy authorized social media platforms to be incorporated into the PSCP process. The second step was what Elo and Kyngäs (2008) would call the organizing phase where I became familiar with the texts by reading and re-reading the documents. Third, I constructed scaffolding to sort and code the material. Schreier (2014) calls this structuring and says it “refers to creating the main categories and generating to creating the subcategories for each main category” [9]. Mayring (2000) argues this phase involves determining the rules, followed by the questions, to help put the material into categories which are continuously revised through feedback loops. Fourth and fifth, I did a first and second round of analysis to move from what were the general themes to of the document to refining particular categories. Schreier (2014) advocates first, “Once all categories have been generated and defined, it is time to take a step back, look at the structure of the coding frame once again, and ‘tidy up’ any loose ends” collapsing and condensing similar categories [10]. Mayring (2000) recommends to work through the texts by going through the materials again and sorting the contents based on the codes. Finally, sixth, I drew conclusions based on the coded scaffolding.

For this article in particular, I went through the documents on a sentence-level basis and identified that there were a number of sentences that expressed concern about the incorporation of social media. I went back and reevaluated the passages expressing concern and further categorized those results. As a result of that analysis, I found the theme of privacy permeated through the hearing. Each step was repeated to make sure the relevant passages were coded according to the definitions, leading me to conclude that Congress was concerned about privacy issues in eight different ways, mostly associated with the content of posts when talking about the incorporation of social media into the PSCP. The conclusions are detailed below.

It is worth noting two points for the analysis and results. First, the statement of Tony Scott, Chief Information Officer of the U.S. Office of Management and Budget summarized policy concerns for the hearing which in addition to privacy concerns, were defending national security, verifying veracity, and considerations of cost and capacity to do this work (Executive Office of the President, Office of Management and Budget [EOPOMB], 2016). I also identified these themes, but I was also able to connect many of these points under the category of privacy concerns as well. Future articles could isolate and critique other specific themes. Second, it is also worth mentioning that despite concerns for the inclusion of social media, Congress was also still supportive of the inclusion. For instance, Congressional representative Mark Meadows commented, “The goal of our background investigations must be to find out if an individual is trustworthy” [11], but although “[b]ack in the 1950s, that meant talking to neighbors and family”, nowadays, “[t]oday, with more than a billion individuals on Facebook, what a person says and does on social media can often give a better insight on who they really are.” Representative Gerald E. Connolly also indicated how a
social media post might useful for demonstrating red flags when he states, that in Facebook postings, “you know, we’re talking about the block party for July in my cul-de-sac. You know, talking about maybe a family reunion and interspersed with all of that, oh, by the way, the President needs to die” [12]. Congressional response was not polarized, however, and even those expressing support also expressed concern. William Evanina, Director of the National Counterintelligence and Security Center in the Office of the Director of National Intelligence argued that “[t]he data gathered via social media will enhance our ability to determine initial and continued eligibility for access to classified national security information and eligibility for sensitive positions” [13] but also voiced concerns for the incorporation. The focus for this paper, however, remains on what was said that related to privacy.

4. Resulting Congressional concerns

Based off an analysis of the hearing, Congress’ concerns for the incorporation of social media in the PSCP were about privacy in eight ways. These categories were: (1) concern for the balance and civil liberties and the 4th Amendment; (2) questions about the retention of information; (3) assurances for authority and policy; (4) concerns about access to information; (5) questions protections for cybersecurity; (6) assurances of successful tests through pilot studies; (7) questions of what information is shared with whom; and, (8) concerns about privacy and discrimination. Table 1 shows the results and a passage from the hearing illustrating each of the themes. Passages were chosen due to their representational and illustrative value.

<table>
<thead>
<tr>
<th>Privacy Concern</th>
<th>Textual Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance and civil liberties and the 4th Amendment</td>
<td>There must be “the right balance between what we need to obtain or should be obtained reasonably from social media in the ever-growing Internet age and balance that with the civil liberties and privacy of our, not only clearance holders, but U.S. citizens” (H. Rep, 2016, p. 23).</td>
</tr>
<tr>
<td>Retention of information</td>
<td>It is important to make sure “that the only collection and retention of data will be what is investigative relevant to completing and authorizing a background investigation” (p. 31) because storage is important for rights to privacy and safety.</td>
</tr>
<tr>
<td>Authority and policy</td>
<td>“I realize that the Federal Government’s authority to collect and review publicly available social media information in the course of a personnel security background investigation and adjudication raises some important legitimate civil liberties and privacy concerns” (p. 5).</td>
</tr>
<tr>
<td>Access (public and private)</td>
<td>“Under this new directive, only publicly available social media information pertaining to the individual under investigation will be intentionally collected” and no other activities will be pursued without national security of criminal reporting requirement (p. 5). This means that there will be no password requests or private account logins for non-public information (p. 6).</td>
</tr>
</tbody>
</table>
| Cybersecurity                                    | But there is still a question of “what are we actually doing to try to
Regarding the retention of information, retention questioned who had authorization to hold the information, asked a question of what was “relevant” information that needed to be retained, and questioned how long that information is stored. Congress was especially concerned with the safety of the storage and concerns that “some enormous government depository of personal information” was going to be created [14]. Information storage complements the next area of concern with is cybersecurity concerns of privacy. Congress wanted to know that if information is being retained, it must be kept safe and secure. This was an especially legitimate concern after the main investigative bureau at the time being hacked several times and exposing the data of over 21 million people (U.S. Government Accountability Office, 2017). Retention and cybersecurity also lead into concerns about what information is shared and with whom, as in, if information is being gathered, it is of concern that there are rules in place detailing whom the data can be shared with and why. The privacy concerns for the category of “authority and policy” aligned with concerns that the government needed to have authorization and verified standards set up so that laws would govern the process and abuse of the collections could be minimized.

Before agencies just started gathering information, though, there were concerns that authorization was granted to everyone and that each agency and authority of the process was recognized. The concerns about public and private access were aligned with just what type of information was being analyzed. Members of Congress wanted to be clear that as per the guidance of SEAD-5, the types of material that would be looked at was a post that is “published or broadcast for public consumption, is available on request to the public, is accessible online to the public, is available to the public by subscription or purchase, or is otherwise lawfully accessible to the public” [15]. Further, Congress wanted clarifications about the directive’s assertions that “the U.S. Government may not request or require individuals subject to the background investigation to provide passwords or login into private accounts or to take any action that would disclose nonpublicly available social media information” [16]. Congress was also concerned that information from pilot studies would be used to show that information could be kept private and that enough resources were being utilized to make the gathering of only public social media both desirable and effective, also making sure to only incorporate truthful information. Finally, there was one thread of concern about the potential for discrimination based on social media information, especially for those with foreign relatives. As foreign contacts are something of
measurement in the PSCP, representative Ted Lieu voiced apprehension that those with foreign connections would be targeted for intense or unwarranted scrutiny, especially concerning their loyalty to the United States if foreign relatives or friends were engaging and visible on one’s social media site.

5. Discussing Congress’ privacy concerns

After the categories of privacy concerns have been identified, it is further useful to answer question two: what do these particular results say about Congress’ conception of privacy? This question moves the argument further by not just seeing what Congress said, but also looking at what the comments could mean. This assessment ends up concluding that Congress did not adequately address the social media organizations that are also stakeholders in the situation which could potentially capitalize on the PSCP process inclusion.

To come to that conclusion, it is useful to see what was, and was not, said during the hearing. First, for what was said, the results do provide empirical evidence that at least Congress is concerned with privacy, and not just for those under the investigative eye, but also friends, acquaintances, or anyone else that might interact in these spaces. The results also show concern about data storage, cybersecurity, the sharing of content, and discrimination. Overall the conclusions about privacy are especially interesting and at least positive points in themselves because they show that members of the U.S. government are not just advocating the inclusion of social media without total disregard for privacy concerns. Despite media criticism that can frame the government as failing to regulate technology (e.g., Feiner and Graham, 2020; Mullin, 2014; Timmons, 2017), this hearing does illustrate the government did have privacy concerns. It would be another question for further research as to what regulations move beyond the hearing and actually show up in formalized policy.

Second, though, the results also illustrate how social media privacy is often approached from primarily the top-layer of content focused on the individual and the government’s control of that surface-level content. The conversation does not turn towards the deeper issues of privacy like Mulligan, et al. (2016) previously mentioned or that Nissenbaum (2011) also mentions in her work on contextual integrity like “cookies, latencies, clicks, IP addresses, reified social graphs, and browsing histories.” Congressional attention is not directed toward the companies who run the platforms who are also stakeholders in the conversation that have the ability to create a deeper, secondary body of content of information by using a user’s movements or metadata. The platforms themselves also need attention for their privacy assurances for this information as the platforms could potentially use or profit from this information, and their potential interaction with government officials in this site could also be a matter a national security.

To illustrate a more platform-oriented question could have been discussed in the hearing, Congress first could have addressed algorithms. One discussed purpose of the hearing was to look at pilot studies to think about incorporating automation and artificial intelligence (AI) so that the public posts could be gathered via third-party companies that operate with private algorithms. As Beth Cobert, Acting Director of the U.S. Office of Personnel Management stated during the hearing:

> OPM issued a request for information seeking to better understand the market and the types of products vendors can provide to meet social media requirements. The RFI [request for information] is in preparation for a pilot that OPM is planning to conduct this year that will incorporate automated searches of publicly available social media into the background investigation process. [18]

Interestingly enough, the algorithms themselves for these automated processes did not seem to be addressed in the hearing. There were no strong concerns about the privacy afforded to the third-party companies or a mention of the algorithm in general other than automation should be tweaked so that only enough information is gathered to keep costs down rather than concerns that third parties would be creating technologies to filter public information in ways that the government may not understand or in ways that might be biased.

Illustrating how this could play out in the real world, the company Lumina advertises itself as a solution for social media checks in background investigations. Lumina advertises their Radiance technology that uses AI and machine learning for OSINT also advertises to have created a solution for federal background investigations that can supposedly identify risky personnel profiles by executing “324,000 queries for each name across all the major search
engines” (Lumina, 2019). If the government hopes to find third-party vendors that can do these checks, algorithms should be a special concern, especially due to problematic assumptions often associated with systems of prediction (Bennett Moses and Chan, 2018; Lepri, et al., 2017). A more technically-oriented question might have also addressed why there should be a sustained inquiry of checks done through mass technical inquiry in the first place rather than have an investigator conduct the check as an individual (which admittedly could bring its own issues).

Second, then, there was also no mention of the effect that the government’s inquiry into one’s particular page, images, content, etc. could also alter one’s social media profile. There was a concern on the privacy of the storage of the content information gathered, but there really wasn’t an inquiry as to a deep connection of a government entity engaging in open source intelligence and showing particular interest in a segment of social media profiles which in theory could have an effect of the underground connections of one’s deeply social profile (although as stated, these connections are deeply private and unknown). Indirectly, large-scale analysis of social media profiles by a particular agency or third party would also potentially be creating a category of users that could be used to identify (at least by the platforms themselves) those that either hold a clearance or are attempting to obtain a clearance, even if in the above-ground content the candidate has not and does not want that information identified. Further, the connections to this person could also be crystalized into a category of users, and this can affect another type of privacy — group privacies as identified by Taylor, et al. (2017) and described by Reviglio and Agosti (2020) as a right “held by a group to safeguard information that is not only private to individuals, but which reveals something about that same group” [19]. This could be problematic if the companies profit for this information, or problematic for national security interests if unauthorized parties gain access to the grouped information.

6. A more macroscopic view

Taking this information a step further helps to answer the paper’s larger question, how could Congress could have overlooked deeper privacy complexities in their critique of the social media incorporation? I offer two explanations. The first explanation involves the complexity of the hearing process, and the second explanation involves simplifying a complex concept to conform to the proceduralized hearing. Both contribute to a better idea of why legislating privacy is so difficult.

6.1. Hearings procedures and the effects on expertise

The first explanation revolves around the nature of a congressional hearing. Hearings are (1) held by subcommittees that must review a variety of topics; (2) are procedurally regulated; and, (3) have a restrictive membership policy. All three elements contribute to a process that doesn’t necessarily cater to expertise. Expertise is often a key piece of deliberation (Renn, 2003). To explain further, first hearings are held by committees or subcommittees that must debate a variety of issues. For this case in particular, of the two subcommittees involved in the hearing, neither was focused specifically on technology. As shown above, the hearing in this case involved two particular subcommittees: (1) Government Operations; and, (2) National Security. Breaking these two groups down, the 114th Government Operations subcommittee reported the following objectives:

- government management and accounting measures, the economy, efficiency, and management of government operations and activities, procurement, grant reform, unfunded mandates, the Office of Management and Budget, federal property, public information, federal records, the federal civil service, the U.S. Postal Service, the Census Bureau, the District of Columbia, and national drug policy. [20]

Alternatively, the National Security subcommittee reported that their objectives in the 114th congressional session were focused on “national security, homeland security, foreign operations, immigration, defense, and criminal justice.” [21]

For both of those subcommittees, there was a wide breadth of topics which were covered, and neither subcommittee focused on technology in particular. It is of note that at the time, there was also a “Subcommittee on Information Technology” that was tasked with “information security management, cybersecurity, information technology policy and procurement, emerging technologies, intellectual property, telecommunications, and privacy,” [22] yet, that
committee was not part of the hearing. It is also of note that in 2019, the Government Operations subcommittee reported the objectives of “federal information technology security, acquisition policy, and management.” [23] but that was not the focus in 2016. In 2016, though, while either committee could cover matters of technology, neither specialized on it. While task variety has benefits, repetition is also valuable for gaining skill in tasks and specialization (Staats and Gino, 2012).

Second, hearings are also procedurally constrained, and often by the chairman, and especially in relation to witnesses who are often the most knowledgeable parties in the hearing. For instance, the rules for the 114th Congress stated “[a] committee member may question witnesses only when recognized by the chairman for that purpose” with a goal of adhering to “the five-minute rule” (with no more than 30 minutes allowed) [24]. Who gets to speak was also monitored, with the chairperson recognizing that speakers are “based on seniority of those majority and minority members present at the time the hearing was called to order and others based on their arrival at the hearing.” [25] Further, the “the chairman shall rule on the relevance of any questions put to the witnesses” with only relevant questions put before witnesses [26]. To prepare for a hearing, it may also be that committee members only got a written statement from a witness only 24 hours prior to their appearance. Further, only witnesses in a non-governmental capacity were required to submit a curriculum vitae elaborating on expertise or disclose of funding by possibly interested parties (Congress.gov, 2015) which might give more context to the testimony provided.

For this particular hearing, there were three witnesses. William Evanina, Director of National Counterintelligence and Security Center, Beth F. Cobert, Acting Director of the U.S. Office of Personnel Management (the agency in charge of the investigation process at the time), and Tony Scott, U.S. Chief Information Officer, U.S. Office of Management and Budget. Each of these three individuals had their own expertise, whether it be Evanina’s involvement in the Director of National Intelligence’s responsibilities “under which the social media directive was developed” [27], Cobert’s in-depth knowledge of the background investigation process, pilots on the inclusion of social media, and the process’ future transition to being handled by the U.S. Department of Defense (U.S. Office of Personnel Management, 2016), or Clark’s extensive technology industry background and his work with the Security and Suitability Performance Accountability Council which coordinates reforms like incorporating social media in background investigations (EOPOMB, 2016). The hearing directives would have consequences, then, because based on the committee rules, it is clear that time is limited, questions are filtered, and one can only speak if formally recognized. It could thus be the case that not every question gets asked and not every member present at the hearing is heard. Further, witnesses might not be able to express every gradation to the debate. Especially with a length of just under an hour and fifteen minutes (C-SPAN, 2016), this hearing could facilitate some argument, but not necessarily a fully nuanced discussion of a topic.

Third, committees in charge of the hearings have restrictive membership policies also controlled by restrictive procedures. According to the U.S. Government Publishing Office (n.d.), a three-step procedure has been put into place for the election of standing committee members, which includes that first, a selection committee from each party caucus recommends members; second, the caucus approves the recommendations, and third, the House approves the recommendations. Subcommittee membership is further reduced, with the committee chairmen assigning members of the subcommittees, restrictions on party ratios, and approval of ranking officials (Congress.gov, 2015). Preference is also given to seniority of the house members and as shown above, the chairmen are also in positions of additional control of duties in the committees.

The set-up of the committees then, doesn’t necessarily mean the most experienced or knowledgeable person available to hear the matter is involved in an issue, and it also doesn’t mean that the chairmen is an expert in the particular issue at hand. For instance in the case of this hearing, according to the hearing transcript, representative Meadows was the chair of the subcommittee on Government Operations, and Ron DeSanits was the National Security subcommittee chair. Neither individuals’ House biographies forefront a strong technology or privacy background (Bioguide, 2021; Bioguide, n.d.). Expertise can be beneficial for leadership (Li, et al., 2016).

6.2. The complexity of privacy and simplification as consequence

Adding to complexities of the hearing process, a second possible reason that could explain why the deeper privacies were overlooked has to do with not only the constraints of a hearing but also the complexity of the concept of privacy in general. As mentioned previously, Congress talked about privacy in eight different ways, with a number of assumptions about privacy, which supports the belief that privacy is hard to define as one simple definition. As Mulligan, et al. (2016) note, though, privacy is a layered concept that has been historically addressed in a variety of ways both in response to both changing technologies and societies.

To talk about privacy, though, almost requires simplicity, but there are various origins that beget this simplicity: (1)
omission from constraints; or (2) omission from non-expertise. Simplification by omission is a result of knowing various ways that privacy can be explained, but due to time, space, or clarity of argument, one must focus on either one or a limited understanding of privacy. For instance, for the hearing, the hearing constraints would limit who is permitted to ask questions and interact with witnesses, and not every question might be addressed in the limited time. Too, in the case of this article itself, using Nissembaum’s theories of contextual integrity were useful for understanding one relevant explanation of privacy, but frames also create terministic screens, which Burke (1984) notes are ways of seeing and not seeing at the same time. When one draws attention to one way of thinking, other ways are left out of focus. Although Nissenbaum (2011) mentions deeper privacy issues, other theories like surveillance capitalism (Foster and McChesney, 2014; Zuboff, 2015) might have also offered another useful lens. Surveillance capitalism (or commodifying personal data) and would have thrust the emphasis to corporations and their various tactics of collecting and sorting data as well as rooted the focus on organizations in legislating privacy in another historical conversation. Regan (1995) noted over 25 years ago, “Yet in policy debates in the United States, the emphasis has been on achieving the goal of protecting the privacy of individuals rather than curtailing the surveillance activities of organizations.”

Simplification from inexperience can also lead to reducing privacy down to only minimal lenses, but the reason for this isn’t necessarily due to external constraints. Instead, this can be due to non-expertise and a lack of privacy literacy. Cultural factors can influence one’s perception of privacy (Cullen, 2009; Westin, 1967), and for instance, one’s location or educational background can change the way one thinks about privacy (Harris, et al., 2003). Fictional movies can also influence the understanding and framing of surveillance (Kammerer, 2012) and thus privacy. One might explain privacy to the full extent of their knowledge despite that privacy might remain a one or few-dimensional concept. While it might be simple to point out government failures based on media headlines, it might also be the case that Congress is not necessarily being purposeful in their omissions. Going back to expertise as mentioned above, the committee that held the hearing did not specialize in technology, so expectations of Congress’ own expertise in the various dimensions of privacy are not assumed. While it would also be naive to assume that Congress wouldn’t think about the various dimensions of privacy and could neglect a robust discussion of platforms, especially in the context of a government hearing where Congress is tasked on assessing its own use of technology, it might not be a stretch to see that Congress wasn’t necessarily attuned to more corporate actions on this particular occasion.

6.3. Why this matters

It is not enough to answer the research questions and end the conversation, though. It is important to also answer why this conversation matters. Each section has led up to the conclusion that Congress did have concerns about privacy, but those worries did not adequately address the involvement of social media organizations. These organizations have the potential to create secondary content not created by the user, and government should at least have a conversation about that. Whether due to the constraints of the hearing, the complexity of privacy, or for some other reason, this paper hopefully at least demonstrates that the process of hearings is complicated and privacy is complex. More specifically, for policy-makers, this paper hopefully draws attention to nuance and the importance of looking at privacy from various lenses. For both for scholars and privacy enthusiasts, this paper hopefully encourages a more nuanced look at government to see government in a variety of situations from the hearings that debate policies to the official laws put in place. While there are some valid criticisms of government’s role in legislating privacy (e.g., Regan, 1995), it is also useful to evaluate what privacy conversations are held and what possible value of these discussions. Lawmaking is complex like privacy, and the two areas put together require tedious examinations into the multiple definitions, processes, and procedures with attention to the degree of simplification.

7. Conclusion

It is the hopes that this argument deepens understanding of privacy by showing how government did try to address privacy issues but also explain how they may have overlooked the deeper privacy complexities that exist for social media, either due to constraints of the process of public debate in government hearings or due to the complex nature of privacy. While it is not wholly practical to use one hearing for one policy in one government program to make large-scale conclusions about all responses to social media’s incorporation into the PSCP, it is useful at least to point out where the government does consider privacy matters when regulating technologies. Future research could engage in looking at how the government does address privacy in other hearings, whether similar privacy protections end up in larger bills or laws, and evaluate how Congress comes to engage with privacy matters. As more technologies are used by governments and society moves towards deep mediatization [29], it is important to think about how privacy is both perceived and regulated by those in positions of power both now and in the future.
About the author

Sarah Young was a LEaDing Fellows Postdoc, Media and Communication, Erasmus University Rotterdam, Rotterdam, Netherlands during the writing of this work. She is now an instructor at the University of Arizona’s School of Information and fellow at the Center for Quantum Networks.
E-mail: sarahyoung [at] arizona [dot] edu

Notes

1. For context, according to Chairman Mark Meadows during the hearing, “Having a security clearance means, by definition, you have access to information that would hurt our national security if it got out, and that is why we perform background investigations on individuals who want a security clearance” (U.S. House of Representatives Committee Repository, 2016, p. 1).


4. It is worth noting though, that some like Thierer (2020) argue that the U.S. Congress is actually a non-actor in tech policy, failing repeatedly to move forward with any substantial policy.


7. Ibid.


17. Nissenbaum, 2011, p. 34.


21. Ibid.

22. Ibid.
23. U.S. House Committee on Oversight and Reform, n.d.
25. Ibid.
26. Ibid.
29. Hepp (2013) defines mediatization as “a concept to capture the interrelation between the change of media and communication on the one hand, and the change of culture and society on the other hand” (p. 615). Hepp (2019) describes that deep mediatization is “the stage of mediatization in which the analysis of algorithms, data and artificial intelligence become crucial to our understanding of the social world”, and there is a whole new level of mediatization taking place below the surface in the depths of media (p. 7). What will come is also “driven forward” by imagination and our visions of the future (p. 3). I would also argue, policy and regulation.

References


P. Mayring, 2000. “Qualitative content analysis,” Forum: Qualitative Social Research Sozialforschung, volume 1,


_____________________

Editorial history

Received 1 February 2021; revised 10 June 2021; revised 15 June 2021; accepted 29 July 2021.

_____________________

This paper is licensed under a Creative Commons Attribution 4.0 International License.

Not too deep: Privacy, resistance, and the incorporation of social media in background checks by Sarah Young.

First Monday, volume 26, number 9 (September 2021).
doi: https://dx.doi.org/10.5210/fm.v26i9.11591