Trump’s position on personal privacy

Food & Diet

In the last paper submitted for this class, various aspects of data security were discussed. The increased probability of cyber-attack and cyber-warfare, the history of data security at the governmental level and what events precipitated data security to be taken more seriously in the first place, and, perhaps most importantly, the importance of a position of coordinator at the White House for the protection of sensitive information. What was concluded in the essay written for the previous prompt about data security regarding this decision of Trump’s was that he either believes that increasing cyber-security measures is not important and would not benefit the nation, or believes that the White House employees can handle cyber-security in a sufficient matter without an expert coordinator position.

Clearly, both of these perspectives are worrying and simply incorrect to hold. Also discussed was Trump’s use of the Congressional Repeal Act to repeal FCC rules passed in 2016 regarding Internet privacy. The conclusion in that discussion was that the decision to repeal such important rules clearly demonstrated that Trump and the administration act on the interests of big businesses rather than the interest and peace of mind of American citizens. This, in essence, is also the overall conclusion that can be made about Trump and the administration’s stance on the issue of personal privacy.

The following paragraphs will discuss the events that have occurred after those discussed in the previous essay for this course, with a focus on privacy at the personal level rather than the governmental level. Ultimately, conclusions will be drawn about the current state of affairs regarding personal privacy, the likelihood of more comprehensive personal privacy laws and the direction they are headed in, how much personal privacy is

valued by the Trump administration, and finally how American citizens feel about personal privacy.

In September of 2018, the Trump administration finally presented a framework addressing consumer data privacy: something many have been waiting for after his repeal of previous laws in the spring of last year. Trump had promised that the next framework would be better for both the consumer and for businesses, as it would be all encompassing as well as fair on the businesses-end; previously, major telecommunications were frustrated by the fact that big websites like Facebook were not required to comply with the same set of rules as the major telecommunication companies.

Also a looming issue over the head of all organizations was (and still is) the fact that there are only state laws about data collection and data privacy but not federal laws. According to an article on Broadcasting and Cable, the new framework actually falls short of Trump’s promise. The way that John Eggerton described the policy was that the administration was presenting broad-brush strokes that would create little to no dispute (Eggerton). He also pointed out that there were no specific measures nor action plan, no specific examples of ways that transparency, control, and security can be increased (Eggerton). The policy failed to mention whether there would be opt-out or, even more protective for the consumer, opt in systems implemented to be the basis of transparency. Therefore, worried consumers are still in the dark regarding the future of personal privacy and frustrated by a policy that is not transparent about the means of promised transparency. As noted in the article, this framework was intended to keep peace between the republicans

and democrats, but only manages to do so because it is so vague: when it becomes time to discuss the specific measures to be taken, the administration will be left back at square 0 and left with a very difficult proposal to re-work.

The National Telecommunications & Information Administration commented on the policy, saying that the policy aims to create “ a reasonably informed user, empowered to meaningfully express privacy preferences, as well as products and services that are inherently designed with appropriate privacy protections, particularly in business contexts in which relying on user intervention may be insufficient to manage privacy risks” (Eggerton). The wording of this is quite ambiguous, as the definition of a reasonably informed user probably varies widely from president Trump to a citizen whose information was compromised in the Facebook data breach, for example. Also, the statement says that products and services should be designed with appropriate privacy protections when Trump has claimed that the new framework will be superior to any from the past (Eggerton). Part 5 of the 7-point plan created says the following: Users should be able to reasonably access and correct personal data they have provided (Eggerton). Again, the word reasonable is being used. Does reasonable mean that it is possible for the consumer to access their personal data they provided, or does it mean that it is easy to access it? Based on the past actions of the administration, the latter does not seem to be the likely scenario. Part 6 reads, Organizations should take steps to manage the risk of disclosure or harmful uses of personal data (Eggerton). Using the word should instead of a word like must is another clear indication that the protection of consumers’

personal data is not being taken as seriously as many are consumers are demanding it be.

This policy draft is likely to cause a lot of conflict between state governments and the federal government. Many states like California, for example, do not have a history of waiting patiently during delays in law making at the federal level. Following the discard of previous protections under the FCC, the state of California created its own set of net-neutrality laws, which required the biggest players of Internet providers like AT&T, Comcast, and Verizon to treat all web traffic equally (Romm, Fung). Just as one would expect, these laws prohibited Internet providers from blocking access to sites and services, slowing down web connections or charging companies for faster delivery of their movies, music or other content (Romm, Fung). But, this was not just another common occurrence of law making at the state level: according to an article written for the Washington Post, some were even calling California’s net-neutrality law the toughest net-neutrality law ever enacted in the United States (Romm, Fung). The way that the Trump administration has handled the personal privacy predicament is likely to result in the same way: states like California are likely to become impatient, and draft a policy that is much more clear but much tougher than one written out by the Trump administration, and therefore not in alignment with the goals of the administration.

Another notably tense relationship regarding governmental stance on personal privacy is that of the U. S. government and the EU. As discussed in the previous essay written for Management of Information Systems, the U. S. and England struggled to work together in the past due to clashing stances

on personal privacy and data security. Both entities had positive intentions on collaborating on a safe-harbor framework, or a private, self-regulating policy and enforcement mechanism that meets the objectives of government regulators and legislation but does not involve government regulation or enforcement (Laudon 137). Under this agreement, U. S. business were allowed to make use of personal data from countries in the EU as long as the EU approved of the privacy protection policies that the U. S. developed (Laudon 137). Ultimately, though, ties were severed when the EU discovered that Facebook’s massive data breach involved compromising data from European citizens as well. Come fall of 2018, and the European Union has arguably created the best personal-privacy law in world history. The law is called the General Data Protection Regulation (GDPR). This law puts emphasis on consent, control, and clear explanations (Tiku).

What is unique about this law is that it no longer permits companies to bring up pages and pages of so-called fine-print, (which no one actually reads) on a user’s screen and then essentially require users to click I agree to use a company’s service (Tiku). The new law requires brief and clear explanations of what is to be collected and, equally as important, why the information is being collected and how exactly it will be used by the company (Tiku). Consumers will have more of a say than ever before, being able to add or omit data held by the company at any time and also being able to limit the use of decisions made by algorithms (Tiku). Is a law mirroring the GDPR likely to be passed in America? Right now, the law protects citizens in every country that is part of the European Union: 28 countries. It is uncertain whether numbers alone are enough to put enough pressure on the U. S. to

pass similar kinds of legislation. Something important to note, though, is that a mismatch in laws of this nature cause a lot of problems for business operating in both the European Union and the United States. Many companies are making its reworked data privacy measures demanded by the GDPR apply across the company on a global scale, as it is simpler than creating different systems (Tiku).

Chief data ethics officer of data-broker company Acxiom, Sheila Colclasure, feels that the GDPR ‘ will set the tone for data protection around the world for the next 10 years (Tiku). If the administration cares about maintaining good relationships with other countries and international organizations, it should follow the same steps. According to the Pew Research Center, consumer confidence about the security of their data has gone down since the rise of the popularity of major social media networks like Facebook. A survey conducted by the research center shows how over 90% of American citizens either selected that they agree or strongly agree that people have lost control over how personal information is collected and used by all kinds of entities (Rainie). In addition, a strong majority of two-thirds have said current laws are not good enough in protecting people’s privacy, and 64% support more regulation of advertisers (Rainie). Based on the outlook of citizens and the administration’s current efforts, it still is uncertain whether the Trump administration will take the opportunity to make a law like the GDPR.