NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

(b) (6)

GDPR

(b) (6)
To: (b) (6)

Fri, Oct 18, 2019 at 12:09 PM

great - thanks.

On Fri, Oct 18, 2019 at 11:52 AM (b) (6) wrote:

> Sure. Here's an extract from our research memo, which I think says this well. I put the whole GDPR paragraph in below, but I think the highlighted portion is the key bit for the footnote - although leave it to you how to reference a footnote in a footnote.
>
> The European Union's AI strategy is nested within its broader emphasis on data privacy, which is most clearly manifested through the GDPR. The GDPR places restrictions on the ability of firms to collect and share personal data without consent, and provides individuals the right to revoke that consent at any given time. This privacy-first approach to data collection and sharing stands in stark contrast with the United States and Japan, which are advocating for more free flows of data. There is evidence that the GDPR has negatively impacted the competitiveness of the EU's tech industry writ large; a recent paper from the National Bureau of Economic Research found that after the rollout of GDPR the number of venture capital deals in the tech industry within the EU declined by 26.1% relative to US-based firms, and the average monetary value of those deals declined by 33.8%.[1] GDPR could prove to be a significant obstacle in any efforts to standardize privacy regulations, which would be a key part of any international data sharing regime.
>
> [1] Jia, J, G Z Jin and L Wagman (2018), "The short-run effects of GDPR on technology venture investment," NBER, Working Paper 25248.

On Fri, Oct 18, 2019 at 11:41 AM (b) (6) wrote:

> (b) (6), at our meeting you basically voiced the footnote I wanted to add on GDPR. Could you write it down? Sorry if you've already done this.
>
> Text:
>
> Allies and partners have told us they are interested in continuing to develop common standards for ethical AI, including in areas such as data sharing, safety, and certification systems for trust and transparency. However, divergent views on data privacy present significant hurdles, in particular with respect to the European Union's General Data Protection Regulation (GDPR). The Commission will explore the implications for AI cooperation in more depth.

--

(b) (6)

Director, Research and Analysis

National Security Commission on Artificial Intelligence

(b) (6)

(b) (6)

The Short-Run Effects of GDPR on Technology Venture Investment

Jian Jia* Ginger Zhe Jin† Liad Wagman‡

November 5, 2018

Abstract

The General Data Protection Regulation (GDPR) came into effect in the European Union in May 2018. We study its short-run impact on investment in new and emerging technology firms. Our findings indicate negative post-GDPR effects on EU ventures, relative to their US counterparts. The negative effects manifest in the overall dollar amounts raised across funding deals, the number of deals, and the dollar amount raised per individual deal.

Keywords: Data, regulation, GDPR, investment, venture financing

JEL Codes: L13, D8, L5, L15, D43

*Stuart School of Business, Illinois Institute of Technology. Email: jjia5@hawk.iit.edu. Jia gratefully acknowledges support from the NET Institute (http://www.netinst.org/).

†University of Maryland & NBER. Email: jin@econ.umd.edu.

‡Stuart School of Business, Illinois Institute of Technology. Email: lwagman@stuart.iit.edu. Wagman gratefully acknowledges support from Data Catalyst (https://www.datacatalyst.org/) and from the Net Institute (http://www.netinst.org/).

1 Introduction

The rise of big data in the global economy has transformed marketplaces, altering the ways in which firms and consumers interact. Individuals are no longer mere consumers of goods, information and services, but public producers of often valuable data. These data have become key inputs in technology-driven innovation, spanning industry sectors from health, advertising, and security, to e-commerce, transportation, and banking. These data are also key inputs in the matching processes among consumers and firms, as well as between firms and other firms. For individual firms, data is a valuable asset to monetize, especially if the data is personally-identifiable, real-time and of high-frequency. Individuals' traits and attributes, their behaviors and online footprints, their comments and photos, their work and leisure habits, and more, are increasingly regarded as business assets that can be used to target services or offers, to provide relevant advertising, financial offerings, and healthcare, or to trade with other parties.

In an effort to leverage the value inherent in the data created by individuals, new services, companies, and markets are emerging. The services, tools, and products being made possible by the increased availability of data are bearing benefits for data subjects and data holders alike. These benefits include tailor-made recommendations, digital personal assistants, new products and offerings, and easy access to previously thin or unavailable markets. The Federal Trade Commission's 2016 report on big data (FTC, 2016) highlights a number of benefits to underserved populations, including increased educational attainment, access to credit through non-traditional methods, specialized health care for underserved communities, and better access to employment.

Despite those benefits, public concerns over the use of personal data have increased. Recent Pew surveys find that 91% of respondents believe they have lost control over how personal information is collected and used, 61% would like to do more to protect their privacy, and 66% said current laws are insufficient for protecting their privacy and would support

more regulation.[1] These concerns are amplified by recent incidences of data breaches and data misuses, and a lack of regulatory actions after these scandals.

Those concerns are not without merit. The Commission's earlier report (FTC, 2014) indicates that data brokers collect and store billions of data elements covering nearly every U.S. consumer, with one data broker holding information on more than 1.4 billion consumer transactions and 700 billion data elements, while another broker added more than 3 billion new data points to its database each month. Another report found that 95% of the top 200 free iOS and Android apps exhibit at least one risky behavior including location tracking, access to social networks, and disclosing the user's personally identifiable information.[2] The FTC's 2016 report also highlights possible risks that could result from biases or inaccuracies about certain groups, including more individuals mistakenly denied opportunities based on the actions of others, sensitive information being exposed, existing disparities being reinforced, increased targeting of vulnerable consumers for reasons such as fraud, an increase in prices for goods and services in lower-income communities, and the weakening of consumer choice.

Against this backdrop, the General Data Protection Regulation was adopted in the European Union on April 14, 2016, becoming enforceable two years later on May 25, 2018. The regulation aims to protect data by 'design and default,' wherein firms are obligated to handle data according to a set of principles and safeguards. GDPR mandates a higher degree of privacy, data management, and control, requires informed opt-in consent for data collection, and assigns substantial liability risks and penalties for data flow and data processing violations. Under the regulation, firms that process personal information must develop protocols to respond to individual data requests within a month, appoint a data protection officer to oversee compliance activities, audit internal data processes, and take proactive

[1] http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

[2] https://www.appthority.com/company/press/press-releases/appthority-exposes-security-and-privacy-risks-behind-top-400-mobile-apps/

steps to anonymize and secure personal data and minimize its collection. In the event of a data breach, organizations must promptly notify the regulator and affected individuals. The regulation requires that users have the rights to access, correct, and erase their personal data, and imposes fines up to 4% of global revenue for any violation.[3]

The enactment of GDPR is particularly likely to influence technology firms, given an ever increasing need for the use of data as a core product input. This study presents an analysis of the impact of the rollout of GDPR on new technology venture investment in the EU. Our findings indicate a negative differential effect on EU ventures after the rollout of GDPR relative to their US counterparts. These negative effects manifest in the overall number of financing rounds, the overall dollar amount raised across rounds, and in the dollar amount raised per individual round. Specifically, our findings suggest a $3.38 million decrease in the aggregate dollars raised by EU ventures per state per crude industry category per week, a 17.6% reduction in the number of weekly venture deals, and a 39.6% decrease in the amount raised in an average deal following the rollout of GDPR.

We then proceed to break down these effects by two crude industry categories and four firm age groups. Somewhat surprisingly, we do not identify particularly different effects for ventures that fall under the healthcare-financial category, despite the existence of arguably stringent regulations that govern data flows in those industries in the US. However, we do find that the negative effects of GDPR on technology investment appear particularly pervasive for nascent, 0-3 year old ventures. We use our results to provide a back-of-the-envelope calculation of a range of job losses that may be incurred by these ventures, which we estimate to be between 3,604 to 29,819 jobs, corresponding to 4.09 to 11.20% jobs created

[3]On June 28, 2018, California adopted a data regulation law (the California Consumer Privacy Act of 2018, A.B. 375) that is set to take effect on January 1 2020. The law, as currently written, would require that firms provide consumers with the ability to port their profiles to other providers, be informed about what personal data are stored about them, why they are collected, request their deletion, and opt out of their sale. The legislation is still subject to amendments, and it is widely understood that the version that was passed is highly likely to change based on input from stakeholders before its implementation in 2020. On November 1, 2018, Senator Ron Wyden's office began circulating a discussion draft of a bill tentatively-named the "Consumer Data Protection Act," which aims to introduce similar and other protections at the federal level.

by 0-3 year old ventures in our sample.

1.1 Literature Review

The literature that examines the implications of data policies and data regulation is growing (Acquisti et al., 2016, offer a recent survey). Goldfarb and Tucker (2011, 2012) examine the effects of the implementation of the EU Privacy Directive and find some evidence that after the Privacy Directive was passed, advertising effectiveness decreased significantly. They argue that digitization means that privacy policy is now a part of innovation policy, an assertion that is in line with our analysis. More recently, Goldberg et al. (2018) examine the impact of the GDPR on online web traffic, sales, and third-party tracking. Using proprietary datasets, they show that for EU firms, recorded pageviews fall by 7.5%, recorded conversions fall 12.5%, and third-party tracking falls 6.2% after the rollout of GDPR.[4] They demonstrate that beliefs about local regulatory strictness plays a factor in firms' reactions. Their results are complementary to our findings. In particular, while their focus is on the health and regulatory compliance of both online publishers and e-commerce sites, our focus is on the broader tradeoff between innovation and data regulation, for which specific considerations such as ad tracking are one of many data monetization components. Moreover, rather than focus on existing firms, our study focuses on emerging ventures that are typically much smaller.

In this regard, our analysis more closely maps the theoretical works of Krasteva et al. (2015) and Campbell et al. (2015), who show that compliance costs and data regulation, respectively, can create barriers to entry and may thus hurt innovation. In particular, Campbell et al. (2015) show that though privacy regulation imposes costs on all firms, it is small firms and new firms that are most adversely affected, particularly for goods where

[4]In a related paper, Tucker (2014) uses a randomized field experiment to show that users are more likely to click on personalized ads once they are given more control over their personally identifiable information, a change that was only driven by the change of user perception of privacy control, as the website did not change how advertisers used data to target and personalize ads.

the price mechanism does not mediate the effect, such as the advertising-supported internet. Krasteva et al. (2015) show that as the costs of compliance by small firms increase, more innovations will be developed within established firms.[5]

As far as health-related data regulation, using variations in state medical privacy laws, Miller and Tucker (2009, 2011) show that privacy regulations restricting a hospital's release of patient information significantly reduced the adoption of electronic medical records. This reduction is costly, as a 10 percent increase in the adoption of such systems can reduce infant mortality by 16 deaths per 100,000 births. A related issue is an insurer's access to information about a person's genetic test results and subsequent price discrimination. In the US, most states have banned the use of genetic information by health insurers; however, some theoretical results show that inefficiencies may arise when test information is private relative to when it is public (Hoel and Iversen, 2002), and some empirical findings identify relationships among how consumers are informed, the control they have over their private information, and whether consumers elect to partake in genetic testing and share their information with providers (Miller and Tucker, 2017).

Data regulation has also been studied in financial markets. Kim and Wagman (2015) theoretically show that an opt-in approach for information trade in financial markets can lead to higher prices, and empirically demonstrate their results in the market for mortgages, with indications of higher mortgage rates, lower mortgage underwriting standards, and potential downstream foreclosures. Pagano and Jappelli (1993, 2002) predict that if banks share information about their customers, they would increase lending to safe borrowers, thereby decreasing default rates. Other studies focus on the effects of credit bureaus and creditor rights using data from a cross-section of countries (see, e.g., Djankov et al. 2007; Qian and Strahan 2007). Hertzberg et al. (2011) and Doblas-Madrid and Minetti (2013) analyze micro data to show that the effect of lenders' information sharing is to reduce incidence of

[5]While one may argue that higher compliance costs may have a positive effect on innovation (e.g., Porter, 1991), Jaffe and Palmer (1997) find little evidence that industries' inventive output (as measured by patent applications) is related to compliance costs.

delinquencies and defaults, but lenders may reduce credit in anticipation of other lenders' reaction to negative news.

The aforementioned works largely examine a specific aspect or implication of data regulation, such as advertising, pricing, defaults in financial markets, and the impact on medical effectiveness. Our work is complementary, in that our analysis centers around the effect of data regulation on technology ventures and the nascent firms that data regulation is most likely to affect. We demonstrate that younger firms are particularly susceptible to the consequences of data regulation. Our findings are thus in line with Kortum and Lerner (2000) who show that the industrial innovations that venture capitalists help facilitate is a multiple of the ratio of venture capital to R&D expenditures, as well as with Kerr et al. (2014), who suggest that the bundle of inputs that angel investors provide have a large and significant impact on the success and survival of new ventures.

The remainder of the paper proceeds as follows. Section 2 describes the data and Section 3 presents the overall empirical approach. Section 4 provides results at the aggregate level, and Section 5 gives sub-sample results broken down by crude industry category and firm age. Section 6 discusses implications for employment and Section 7 concludes.

2 Data

Our primary data source is Crunchbase, a platform for tracking information about technology businesses, particularly nascent ventures.[6] We collect data on all technology-venture related activity in the EU and US from July 2017 to September 2018, including the parameters of venture financing rounds, such as venture information (name, location, operating category, founding date, financing dates, and a range on the number of employees) and funding information (the size of the funding round in USD, the date each round was announced, the type of financing round such as seed, Series A, Series B, and the number, names, locations, and

[6]For recent activity in the academic literature that pertains to this data source, see Hochberg (2016), Kaplan and Lerner (2017), Lerner et al. (2018), and Chatterji et al. (2018).

types of the participating investors). Each venture in the dataset is also tagged with a few relevant product keywords (e.g., 'software', 'e-commerce', 'finance', etc).

We treat each funding round observed as a 'deal' event, tallying deals per week in each crude industry category and in each US state or EU member state (henceforth, state).[7] Since each deal is tagged with product keywords, we further group ventures into either healthcare-financial or other technology. We choose to group the data into these two crude categories, partly because healthcare and finance are subject to industry-specific regulations in the US,[8] thus comparing them against other technology firms allows us to detect a potentially differential effect of GDPR on healthcare-financial firms. Another reason is that the industry mix of ventures varies greatly across states, but every state has at least one deal in each of the two crude categories throughout the sample. Hence, the two-category grouping helps us construct a balanced sample at the aggregate level by week, state and category. We further collect local macroeconomic controls such as unemployment rate, CPI, interest rate, and GDP, for each state in which a venture is located.[9]

Table 1 reports the summary statistics at the aggregate level in the EU and US. Panel A indicates that our sample comprises 24 EU member states. On average, both the weekly dollar amount raised (in millions) and the number of deals per state per category are similar between the EU and US. Panel B reports summary statistics for each of the two categories we track. Figure 1 depicts weekly trends for the number of deals and dollar amount raised for the EU and US. From both the aggregate and average aspects, there are no noticeable differential trends in the EU and US.

[7]Despite Brexit, we include Great Britain as part of the treatment group due to its adoption of a GDPR-like regulation in the same time frame as the rest of the EU, and due to the fact that it is still bound by GDPR during our sample. In addition, the few observations we have for Bulgaria, Cyprus, Malta, and Lithuania are removed because some macroeconomic variables were not available for those member states at monthly frequencies.

[8]In the US, the Health Insurance Portability and Accountability Act (HIPPA) governs data collection, data use and data security for health care, and the Gramm-Leach-Bliley (GLB) Act governs similar issues for finance.

[9]For a few months in 2018 for which macroeconomic data was yet available (August and September for CPI and unemployment; July through September for GDP), we extrapolated macroeconomic variables by using their corresponding growth averages from 2017 and 2016.

At the individual-deal level, we remove observations with missing dollar amounts or missing funding types (e.g., 'angel', 'seed', 'Series A', etc).[10] We calculate a venture's time-variant age based on its founding date.[11] We consider four different age categories: new firms (0-3 years old), young firms (3-6 years old), established firms (6-9 years old), and mature firms (9+ years old). Firms may consequently switch between age categories in our sample. We also group deals, based on their funding type group, into three unique funding stages of pre-stage, main-stage, and late stage.[12]

Summary statistics at the deal level are also in Table 1. Panel C of the table indicates that the average dollar amount raised per deal is similar (about $22 million) in the EU and US in our sample. Its distribution is highly skewed in both the EU and US, with the median dollar amount raised per deal ($1.42 million for the EU and $3 million for the US) much lower than the average. The average firm age is about 3 years in both the EU and US when excluding mature (9+ year old) firms. Category-specific deal-level summary statistics are presented in Panel D, where it can be seen that the average funding size for a healthcare-financial venture is larger in the EU than in the US. Panel E suggests that most funding deals take place in either the pre-stage or in the main stage. Panel F provides information about the distribution of firm ages in our dataset. While they are similar, the US has a larger proportion of 9+ year old firms. The EU, in contrast, has a larger proportion of firms in the 0-3 and 3-6 age groups, firms which may be particularly susceptible to an increase in the costs of compliance. Of particular interest is the fact that close to 70% of technology ventures in the EU and US in our sample are relatively young, 0-6 year old ventures. It is

[10]There are 21,726 deal observations in the overall sample. Of those, 4,358 observations are missing dollar amounts and an additional 175 observations are missing funding types, which together amount to about 20% of the overall sample. Dollar-amount specifications thus use 17,192 observations; number-of-deals specifications use the full sample comprising 21,726 observations.

[11]There are some cases where a founding date is unavailable or when a venture's first financing round predates its founding; in those cases, we use the venture's first financing round as its founding date.

[12]Specifically, we group angel, seed, pre-seed, convertible note, and product crowdfunding into pre-stage, we group series A, B, C, bridge series A-B, initial coin offering, and equity crowdfunding into the main stage, and we group series D and later, private equity, debt financing, and other post IPO activities into the late stage. The precise grouping of funding types does not change the nature of the results.

also apparent that the older the firm, the higher the average dollar amount raised per deal.

3 Empirical Approach

We aim to study the effects of the rollout of GDPR in May 2018 on venture financing in the EU. We do so by contrasting venture activity in the EU with the US before and after the rollout of GDPR. While GDPR was enacted in April 2016, its enforceability began to take hold in May 2018, with mandatory implementation by EU member states and mandatory compliance by firms. Our hypothesis is that as GDPR's enforceability came into place, entrepreneurs and investors both realized the actual compliance and implementation costs, as well as the ex-post implications of GDPR. This is particularly evident in the month immediately before the GDPR effective date, as major platforms like Google, Facebook, Amazon, and Apple, on which a vast number of technology ventures rely, began to reveal the ways in which they were tightening their platforms and app stores with new data sharing, data portability, and data liability rules.[13]

We test the effect of GDPR using a difference-in-differences methodology (DID). We carry out the empirical analysis at two levels. At the aggregate level, each observation is defined by week-state-category, while the dependent variables are either the total dollar amount raised across all deals in that week-state-category, or the number of deals reached in that week-state-category. Both could be zero if no venture in the state had any deal in that week-category. At the deal level, the sample includes every deal that has non-missing amount raised and

[13]Examples include SafeDK in 1/25/18 documenting that more than half of mobile applications are not GDPR ready (https://www.mobilemarketer.com/news/study-55-of-apps-may-not-meet-gdpr-privacy-standards/515546/), and numerous examples from May 2018. Those include Apple reportedly removing apps that share location data (https://www.idownloadblog.com/2018/05/09/apple-removing-apps-location-data/) and updating its privacy terms (https://techcrunch.com/2018/05/23/apple-introduces-new-privacy-portal-to-comply-with-gdpr/), Facebook announcing that "Businesses may want to implement code that creates a banner and requires affirmative consent? Each company is responsible for ensuring their own compliance" (https://developers.facebook.com/ads/blog/post/2018/05/10/compliance-protections-gdpr/), Shopify updating its app permissions for merchants and developers (https://www.shopify.com/partners/blog/gdpr-compliance), Google releasing new consent requirements to developers (https://bit.ly/2ziUgJA), all shortly before GDPR took effect on May 25, 2018.

non-missing funding types. By definition, the dependent variable (amount raised per deal) is always positive. Since both levels of analysis use samples derived from the same raw data, we consider the total dollar amount raised per week-state-category an overall metric of venture investment, which encompasses an extensive margin (total number of deals per week-state-category) and an intensive margin (amount raised per deal conditional on having reached a deal).

Our treatment group comprises EU ventures and our control group comprises US ventures. While the treatment group does have lower levels of venture activity than the control group, there does not appear to be a differential pre-trend that would violate the common trend assumption in our DID analysis. At the aggregate level, Figure 1 depicts trend lines of the weekly total amount raised in the EU and the US, the weekly total number of deals in the EU and the US, the average amount raised per week-state-category, and the average total number of deals per week-state-category from July 2017 to September 2018. All four subfigures suggest that some sustained divergence took place between EU and US ventures around the time that GDPR came into effect. Both EU and US trends also track each other closely otherwise, and particularly so up until May 2018. At the deal level, Figure 2 confirms that there are no differential trends between the EU and US in the frequency of deals or in the average dollar amount raised per deal.

For aggregate-level analysis, the specification is given by:

$$y_{sct} = \alpha_s + \alpha_c + \alpha_t + \delta X_{st} + \beta GDPR_{sct} + \varepsilon_{sct},$$

where s denotes state, c denotes category, t indexes week, $GDPR_{sct}$ indicates whether the state s is located in the treatment group (EU) and subject to GDPR at time t. Y_{sct} is the dependent variable of interest, which is either the total dollar amount raised or the number of financing deals in each week-state-category. Week, state and category fixed effects are denoted by α_t, α_s and α_c, respectively, whereas X_{st} are state-specific macroeconomic control

variables (monthly unemployment rate, CPI, interest rate, and quarterly GDP), and ε_{sct} is an error term. We use a Tobit specification censored at 0 for dollar amount regressions because we only observe deals that go through. We use a Poisson specification for the number of deals regressions due to a relatively large number of zeroes at the week-category-state observation level. In all cases, we obtain similar results with OLS.

At the aggregate level, the coefficient β captures the effect of GDPR across both categories. Standard errors are clustered at the state level, because the GDPR requires state-specific enforcement and the heterogeneity is confirmed in market perception.[14]

Figure 3 depicts coefficient plots of the monthly pre-treatment tests for the number of deals and dollar amount raised using Poisson and Tobit specifications, respectively. To perform pre-treatment tests, we run the same specification for the pre-GDPR data, including a full set of interactions between the dummy of EU and each monthly dummy. The coefficients of these interactions are shown in the figures, along with their confidence intervals. Figure 3(a) shows that there is no pre-existing differential trend between the EU and US in the number of deals before May 25, 2018, confirming the observable trends in Figures 1(a) and 1(c). Figure 3(b) suggests there is no pre-existing differential trend between the EU and US in the aggregate dollar amount raised per week before April 30, 2018. It is possible that due to some of the major platforms announcing their data-related policy changes in early May 2018, some market movement may have taken place earlier than May 25. As robustness checks, we report the results excluding May 2018 and they are largely unchanged. For heterogeneous effects by category, we apply the same specification to healthcare-financial

[14]Despite GDPR applying to all EU countries, the policy change is at the state level. This follows from the definition of the 'lead supervisory authority,' which has the "primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data." The location of the lead supervisory authority is based on a firm's main establishment location. Recital 127 further states that: "Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State." Goldberg et al. (2018) additionally demonstrate that GDPR suffers from implementation heterogeneity across EU countries, heterogeneity that lines up with traditional member state enforcement behaviors.

and other technology separately. For heterogeneous effects by firm age, we reorganize the aggregate data by week, state and firm age (0-3, 3-6, 6-9, 9+). We then apply the same specification to each group of firm age separately.

For each aggregate-level regression, we perform pre-treatment tests by quarter. To conduct such tests, we run the same specification using pre-GDPR data only, include interactions between the EU dummy and quarterly dummies (2017Q4, 2018Q1, 2018Q2 while 2017Q3 is the default), and test whether the coefficients of these pre-treatment interactions are jointly zero.[15] The test-statistics is never significant above the 90% confidence level. In few cases, the pre-treatment test gets close to be significant at the 85-90% level, mostly because the negative effect of GDPR started to appear a few weeks before May 25, similar to what we have shown in Figure 3(b). For this reason, the reported estimate of β is likely a conservative estimate of the true effect.

At the deal level, we use the specification:

$$ln(y_{jsct}) = \alpha_s + \alpha_c + \alpha_t + \delta X_{jsct} + \beta GDPR_{jsct} + \varepsilon_{jsct},$$

where j identifies deals according to their assigned unique identifier, the dependent variable $ln(y_{jsct})$ is log of the dollar amount raised in deal j, X_{jsct} denotes deal-level variables such as funding type, investor type, and firm age, α_t, α_s, and α_c are week, state and category fixed effects, $GDPR_{jsct}$ is a dummy variable that equals one after May 25, 2018 if applicable to deal j in state s and zero otherwise, and ε_{jsct} is an error term. We use the log of the amount raised per deal because the amount raised is always positive but its distribution is highly skewed. As a robustness check, we also report results that top-code the amount raised at the 95 percentile of the sample. The same specifications apply to the subsamples by category and by firm age. In all regressions, we cluster the error term by state.

[15] We test quarterly instead of monthly or weekly interactions because the more we zoom in a particular subsample, the more spontaneity there is in a short time window. Quarterly gives us a reasonable time frame to average over these idiosyncrasies, across all types of samples.

4 Overall Effects of GDPR

We begin by examining how the aggregate weekly dollar amount for each state in each category changes from the pre to the post period of the implementation of GDPR. Column 1 of Table 2 reports the results of our baseline specification. We focus on the *marginal* effects computed from the estimated coefficients of GDPR according to the Tobit specification. It can be seen that on average, each category in each EU state incurs a $13.90 million decrease after the rollout of GDPR. In Column 2, we right censor the weekly aggregate dollar amount at the 95-percentile value ($175 million) to reduce the influence of outliers. Column 2 suggests that each category in each EU state, after top coding, experiences a $3.38 million decrease following the rollout of GDPR. The effects do not change when adding a linear trend (column 3 of Table 2).

As previously indicated, our pre-treatment tests suggest that the effect of GDPR's rollout on EU ventures may have started earlier in May. Column 4 demonstrates that when May is excluded, the estimated effect is even stronger, suggesting a $4.49 million decrease in the aggregate dollar amount per state per category after the rollout of GDPR. Using an OLS specification, Column 5 indicates that the aggregate dollar amount for each state in each category faces a 26.5% decrease after the rollout of GDPR. This marginal effect on dollar amount is computed from the estimated coefficient of GDPR, accounting for the fact that the dependent variable is log of one plus the dollar amount.

The aggregate dollar amount estimation combines extensive margin (number of deals) and intensive margin (dollars raised per deal) effects. To decompose them, we estimate the effect of GDPR's rollout on the number of deals per week-state-category, and on the dollar amount per deal. Since the number of deals per week-state-category is an integer count (including zero) but the dollar amount per deal is always positive, we use a Poisson specification for the former (at the aggregate level) and the log linear specification for the latter (at the deal level).

Table 3 reports the effect of GDPR's rollout on the aggregate number of deals. We focus on the *marginal* effects computed from the estimated coefficients of GDPR according to the Poisson specification. Our baseline model suggests a 17.6% decrease in the number of EU venture deals. Column 2 adds a linear trend to the baseline specification, and Column 3 excludes May observations. Both specifications give similar results (in the case of Column 3, excluding May gives a greater decrease of 22.82%). An OLS specification with the dependent variable of $ln(1 + \#$ of deals) in Column 4 indicates a 9.07% decrease. The marginal effect on the number of deals is computed from the estimated coefficient of GDPR, accounting for the fact that the dependent variable is log of one plus the number of deals.

Table 4 provides the results of the deal-level log linear specification. Our baseline model in Column 1 suggests a 39.6% decrease in the dollar amount per deal after the rollout of GDPR. Column 2 summarizes a similar estimation when right censoring the sample at the 95-percentile level, and suggests a similar reduction of 38.0%. Column 3 adds a linear trend and Column 4 excludes May from the sample; the results are similar in both cases.

5 Heterogeneous Effects of GDPR

While the overall effects we measure may be negative and statistically significant, there may exist heterogeneity both at the aggregate level and at the deal level in the effects across firm technology category types and firm age groups. This section applies the baseline specification to some of these subsamples. An example of such heterogeneity is presented in Figures 4 and 5, where the weekly trends of the number of deals and dollar amounts for the EU and US are plotted separately for healthcare-financial and other technology. There is no apparent differential trend between the EU and US prior to May 2018, and GDPR seems to have had effects in both category groups. Figure 4 in particular demonstrates that the sample comprises some significant outliers and, as such, right-censoring the data to mitigate the impact of outliers on our dollar amount estimations is likely necessary.

Table 5 reports the baseline model specification for the number of deals, the aggregate dollar amount raised (with right censoring at the 95-percentile level), and the dollar amount raised per deal for healthcare-financial and other technology, respectively.

Columns 1, 3 and 5 of Table 5 indicate that GDPR had negative effects on the number of deals, the aggregate dollar amount raised, and the dollar amount raised per deal by EU ventures in the healthcare-financial category. The three columns suggest a decline in the number of deals of 18.86% and reductions of $5.22 million and 56.6% in the aggregate dollar amount per week and in the dollar amount per deal, respectively. For the group comprising all other technology, Columns 2 and 6 suggest large negative effects for the number of deals and dollar amount per deal; however, the effect on the aggregate dollar amount per week is insignificant in Column 4. We believe this is possibly because of a large standard deviation on the aggregate dollar amount per week in this rather broad category.

The somewhat comparable negative effects on ventures in healthcare-financial versus other technology may be perceived as surprising, in light of the seemingly stringent healthcare and financial data privacy laws in the US (HIPPA and GLB). However, those laws are arguably older and systems to comply with them have been in place for a number of years. Moreover, HIPPA, for instance, allows providers to require consent prior to providing services, a requirement that GDPR explicitly prohibits. GLB, for instance, adopts an opt-out approach, where information is collected by default and consumers have a limited ability to opt out. GDPR, in contrast, mandates an informed opt-in consent for each type of data collected, and further requires data management, data auditing and classification, data risk identification and mitigation, and data interfaces for users to easily obtain their own data and request that it be deleted. GDPR also imposes substantially larger penalties of up to 4% of a firm's global revenues. Hence, our results potentially indicate that GDPR is widely transformational across the technology sector in a rather broad way, even when compared to existing strict data regulations of US firms.

Another example of subsample heterogeneity is presented in Figures 6 and 7, where the

average weekly number of deals and aggregate dollar amount raised, respectively, are depicted for four different age groups of EU and US ventures. Similarly to the preceding analysis, we also examine the heterogeneous effects of GDPR across these firm age groups. Under the aggregate dollar amount per week specification, when examining subsamples according to firm age groups, Column 1 of Table 6 suggests that GDPR had a negative effect on the aggregate dollar amount invested per week in the new (0-3 year old) firm subsample, with a reduction of $0.9 million per week. Columns 2 and 3 indicate insignificant effects for firms in the 3-9 year old age group, and Column 4 indicates a larger negative effect of $7.1 million per week for firms in the 9+ year-old age group. Under the number of deals per week specification, Table 7 presents similar findings. Columns 1 and 4 indicate significant reductions in the number of deals for firms in the 0-3 and 9+ year-old subsamples of 19.02% and 29.53%, respectively, and Columns 2 and 3 indicate insignificant effects for firms in the intermediate (3-9 year old) subsamples.

At the deal level, Column 1 of Table 8 suggests a negative effect under the deal-level dollar amount specification for firms in the 0-3 year old subsample, with a reduction of 27.1% per deal. Columns 2 and 3 suggest negative effects for firms in the 3-6 and 6-9 age groups, with reductions of 31.4% and 77.3%, respectively. Due to the absence of significant aggregate effects for these age groups in terms of the weekly number of deals and total dollar amounts invested, we believe these reductions may be the result of the more sporadic nature of deals for firms in these age groups.[16] Column 4 indicates an insignificant deal-level effect for the subsample comprising 9+ year-old firms.

Ventures in the 0-3 year old group in our sample are those ventures that primarily seek seed, series A and series A-B bridge rounds, as indicated in Figure 8 — rounds where angel investment and venture capital begin to overlap for the first time, with venture capital replacing funding that was previously raised from angel investors. In the figure, the circles

[16]Firms in the 0-3 age group comprise 46% of our observations, whereas 3-6 year-old firms comprise 28%, and 6-9 year-old firms comprise 10.5%.

depict the relative numbers of observations, with larger circles indicating more deals. The numbers of seed, Series A, and Series A-B deals in Figure 8(a) for 0-3 year old firms are significantly larger than their corresponding numbers in Figures 8(b)-8(d) for 3+ year-old firms. The combined estimates of Tables 6 through 8 thus suggest that those nascent firms that most critically depend on angel investment as well as those firms that are in the process of making the transition from angel investment to venture capital are particularly susceptible to a negative effect from GDPR.

6 Implications for Employment

For each venture, our dataset provides a range on the number of employees (e.g., 1-10, 10-50, 50-100, etc). However, this range is time-invariant as of the composition time of our dataset, October 1, 2018; thus, we do not have historical ranges. In other words, as of October 1, 2018, we have the total dollar amount raised by each firm and a range on its current number of employees. We can use this information to provide a back-of-the-envelope measure of the average dollar amount raised per 'current' employee as a function of the firm's age. We focus on new (0-3 year old) ventures, because the literature has demonstrated that they tend to be the primary job creators,[17] and we focus our analysis on EU ventures to assess the potential for EU technology job losses as a result of GDPR.

To provide a back-of-the-envelope calculation of the effect on jobs, we calculate the average dollar raised per deal and the total number of deals in the post-GDPR period by 0-3 year old ventures. Columns 4 and 5 of Table 9 show our calculations. In the third quarter of 2018, 0-3 year old ventures raised on average $3.32 million per deal, with 690 deals made by 0-3 year old ventures. Once the estimated reduction in the dollar raised per deal and the reduction in the number of deals are applied to those firms' totals, the predicted overall dollar amount suggests a $1589.77 million decrease for 0-3 year old firms. This is corroborated at

[17] See, e.g., Haltiwanger et al. (2013).

the aggregate level when using estimates of the change in the total weekly dollar amount invested per state per category to estimate the decrease in the aggregate amount invested in 0-3 year-old EU firms after GDPR, suggesting $1217.70 million decrease for 0-3 year old firms, in line with the first approach. To extrapolate these losses to an entire calendar year, we examine the ratio of EU venture activity in June through September 2017 to the rest of calendar year 2017 for new ventures, and apply the same multiplier to these totals.

To identify the average bounds on the annualized dollar amount raised per employee, we focus on EU ventures founded on or after 2015. An advantage of focusing on 0-3 year old firms is that our dataset can provide their total amounts raised since their founding. The average age for ventures in this group is 1.21. For each firm in this group, its total dollar amount raised is divided by the bounds on its employee range, which provides a lower and upper bound on its total dollar amount raised per current employee. We then obtain the average lower and upper bounds across this subsample and divide it by the average firm age to obtain a crude back-of-the-envelope calculation of the dollar amount raised per employee per year. This calculation gives an average lower bound of $0.123 million and an average upper bound of $1.02 million for 0-3 year old firms.

We can use these average annualized bounds of dollar amount raised per employee and the estimated annual investment losses following the rollout of GDPR to obtain a back-of-the-envelope estimate of the number of technology venture jobs lost in the EU. We obtain a lower bound of 4,705 jobs lost and an upper bound of 38,931 jobs lost from our first approach (using the number of deals times the dollar amount per deal), and a lower bound of 3,604 jobs and an upper bound of 29,819 jobs by using the total dollar amount approach. We tally up the ranges of employees for all firms founded since 2015 in our sample.[18] Using the approach based on the aggregate dollar amount invested, as a percentage of the total

[18]Firms that are missing employee ranges in the subsample are counted by assuming they have the subsample average employee range. This may mean that our results are understated since some of those firms may have ceased operating. Constructing the subsample with firms founded on or after January 2015 may also understate our results since some of those firms may be entering their fourth year of operation in 2018.

range on employment by EU ventures in the subsample comprising firms in this age group, the estimated job loss bounds translate to a 4.09%-11.20% loss in the number of individuals employed by those firms.

7 Conclusion

We presented analyses of the short-term effects of the rollout of GDPR on investment in technology ventures. We found evidence suggesting negative and pronounced effects following the rollout of GDPR on the number of venture deals, the size of those deals, and the overall amount of dollars invested. We broke down those effects according to two venture categories and four venture age groups, and presented a rough estimate of the effect on the number of jobs for 0-3 year old technology ventures.

It is important to emphasize that our dataset is not a complete universe of venture funding, but rather a partial snapshot of primarily venture capital and angel investments in technology ventures. As such, our results must be taken with a bit of caution, given that the effects we observe may be incomplete. At the same time, our findings indicate that it is exactly those nascent ventures that are in the process of transitioning from angel to venture capital that may be most impacted by GDPR.

Another caveat is that the impact estimated on EU ventures is relative to their US counterparts. To the extent that capital flows freely across continents, it is unclear whether the reduced investment in the EU may have in tandem translated to additional support for US ventures or that it reflects the reluctance by investors to invest anywhere. If it is the former, our estimates may have overestimated the effects of GDPR; if it is the latter, our estimates may be conservative as our sample does not include ventures that could serve EU residents but are based in other countries.

While our analyses concern the amount of dollars invested in technology, they are not necessarily translatable into welfare implications. For instance, a reduction in investment

dollars in technology ventures could benefit welfare if firms that are potentially harmful from a societal perspective do not come to fruition. Similarly, it could be that data regulation encourages new types of innovation further down the road.

It is also important to emphasize that given our data, our measure of the effect on jobs can only provide rough back-of-the-envelope ranges on job loss estimates. This is because, on the one hand, we have no insight into whether investors are taking a wait-and-see approach nor do we know the outside options of affected firms or of those individuals who would have been employed by the firms in our dataset had it not been for GDPR. There may also be jobs created as a result of GDPR (for instance, data privacy compliance officers, data security and management ventures, etc). On the other hand, the potential for job losses may well extend and intensify past our four months post-GDPR dataset period, in which case the effect on jobs is understated. Moreover, our estimates do not incorporate potential foregone related job creation (for instance, downstream jobs to service the additional employees that may have been employed had it not been for the rollout of GDPR). The long-term impact of GDPR on the EU technology venture scene will become clearer in the years ahead.

References

[1] Acquisti, A., C. Taylor, and L. Wagman (2016): "The economics of privacy," *Journal of Economic Literature*, 54(2), 442–492.

[2] Bertrand, M., E. Duflo, and S. Mullainathan (2004). "How much should we trust differences-in-differences estimates?" *Quarterly Journal of Economics*, 119(1), 249–275.

[3] Campbell, J., A. Goldfarb, and C. Tucker (2015): "Privacy regulation and market structure," *Journal of Economics & Management Strategy*, 24(1), 47–73.

[4] Chatterji, A., S. Delecour, S. Hasan, and R.M. Koning (2018). "When does advice impact startup performance?" *NBER Working Paper*.

[5] Djankov, S., C. McLiesh, and A. Shleifer (2007): "Private credit in 129 countries," *Journal of Financial Economics*, 84(2): 299–329.

[6] Doblas-Madrid, A., and R. Minetti (2013): "Sharing information in the credit market: Contract-level evidence from U.S. firms," *Journal of Financial Economics*, 109(1), 198–223.

[7] Federal Trade Commission (2014): "Data brokers: A call for transparency and accountability." Accessible at *https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014*.

[8] Federal Trade Commission (2016): "Big data: A tool for inclusion or exclusion?" Accessible at *https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.*

[9] Goldberg, S., G. Johnson, and S. Shriver (2018): "Regulating privacy online: An early look at Europe's GDPR," *Working paper*.

[10] Goldfarb, A., and C.E. Tucker (2011): "Privacy regulation and online advertising," *Management Science*, 57(1), 57–71.

[11] Goldfarb, A., and C.E. Tucker (2012): "Privacy and innovation," *Innovation Policy and the Economy*, 12(1), 65–90.

[12] Haltiwanger, J., R. S. Jarmin, and J. Miranda (2013): "Who creates jobs? Small versus large versus young," *Review of Economics and Statistics*, 95(2), 347–361.

[13] Hertzberg, A., J. Liberti, and D. Paravisini (2011): "Public information and coordination: Evidence from a credit registry expansion," *Journal of Finance*, 66(2), 379–412.

[14] Hochberg, Y.V. (2016). "Accelerating entrepreneurs and ecosystems: The seed accelerator model," *Chapter in NBER book Innovation Policy and the Economy*, 16(2016), 25–51.

[15] Hoel, M. and T. Iverson (2002): "Genetic testing when there is a mix of compulsory and voluntary health insurance," *Journal of Health Economics*, 21, 253–270.

[16] Jaffe, A.B. and K. Palmer (1997): "Environmental regulation and innovation: A panel data study?" *Review of Economics and Statistics*, 1997: 610–619.

[17] Kaplan, S.N. and J. Lerner (2017): "Venture capital data: Opportunities and challenges," *Measuring Entrepreneurial Businesses: Current Knowledge and Challenge*.

[18] Kerr, W.R., J. Lerner, and A. Schoar (2014). "The consequences of entrepreneurial finance: Evidence from angel financings," *Review of Financial Studies*, 27(1), 20–55.

[19] Kim, J.-H. and L. Wagman (2015): "Screening incentives and privacy protection in financial markets: A theoretical and empirical analysis," *RAND Journal of Economics*, 46(1), 1–22.

[20] Kortum, S. and J. Lerner (2000): "Assessing the contribution of venture capital to innovation," *Rand Journal of Economics*, 31(4), 674–692.

[21] Krasteva, S., P. Sharma, and L. Wagman (2015): "The 80/20 rule: Corporate support for innovation by employees." *International Journal of Industrial Organization*, 38: 32–43.

[22] Lerner, J., A. Schoar, and S. Sokolinski (2018). "The globalization of angel investments: Evidence across countries," *Journal of Financial Economics*, 127(1), 1–20.

[23] Miller, A.R. and C.E. Tucker (2009): "Privacy protection and technology diffusion: The case of electronic medical records," *Management Science*, 55(7), 1077–1093.

[24] Miller, A.R. and C.E. Tucker (2011): "Can health care information technology save babies?" *Journal of Political Economy*, 119(2), 289–324.

[25] Miller, A.R. and C.E. Tucker (2017): "Privacy protection, personalized medicine, and genetic testing," *Forthcoming Management Science*.

[26] Pagano, M. and T. Jappelli (1993): "Information sharing in credit markets," *Journal of Finance*, 48(5), 1693–1718.

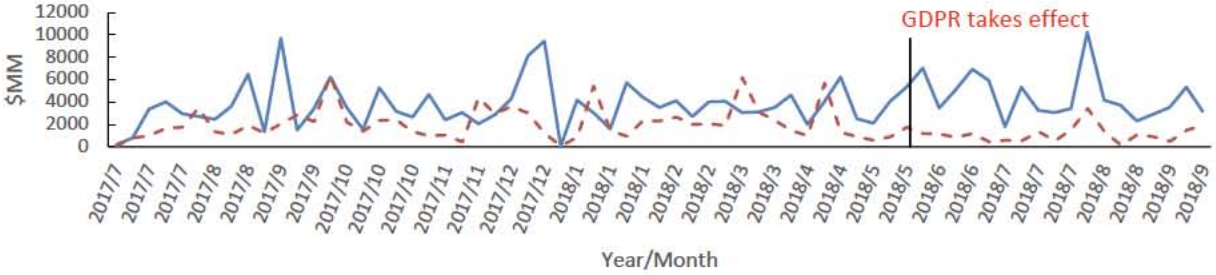
[27] Pagano, M. and T. Jappelli (2002): "Information sharing, lending and defaults: Cross-country evidence," *Journal of Banking and Finance*, 26(10), 2017–2045.

[28] Porter, M.E. (1991): "America's green strategy," *America's Green Strategy*, 264(4), 168.

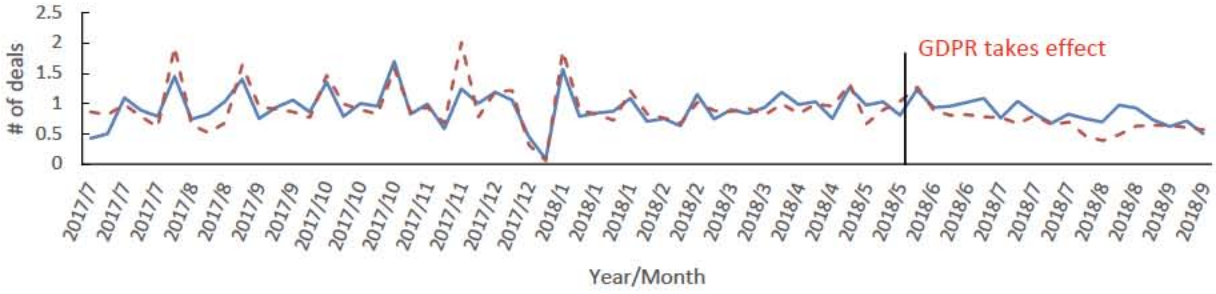
[29] Qian, J., and P. Strahan (2007): "How laws and institutions shape financial contracts: The case of bank loans," *Journal of Finance*, 62(6), 2803–2834.

[30] Tucker, C.E., (2014): "Social networks, personalized advertising, and privacy controls," *Journal of Marketing Research*, 51(5), 546–562.

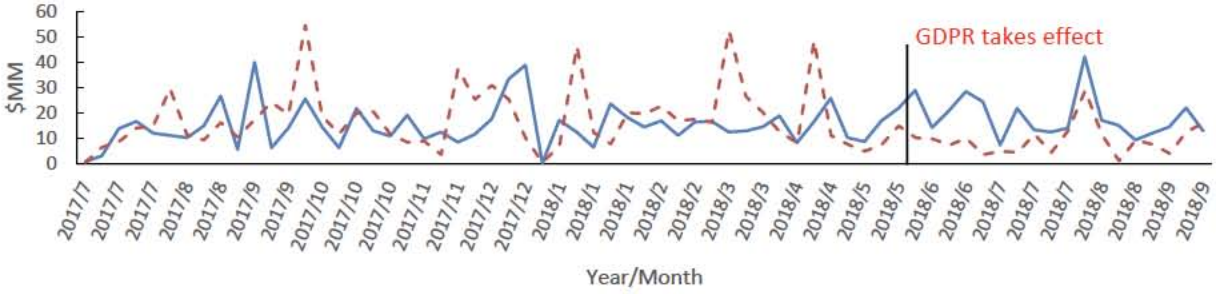
(a) Total # of deals per week between EU and US



(b) Total $ amount raised per week between EU and US

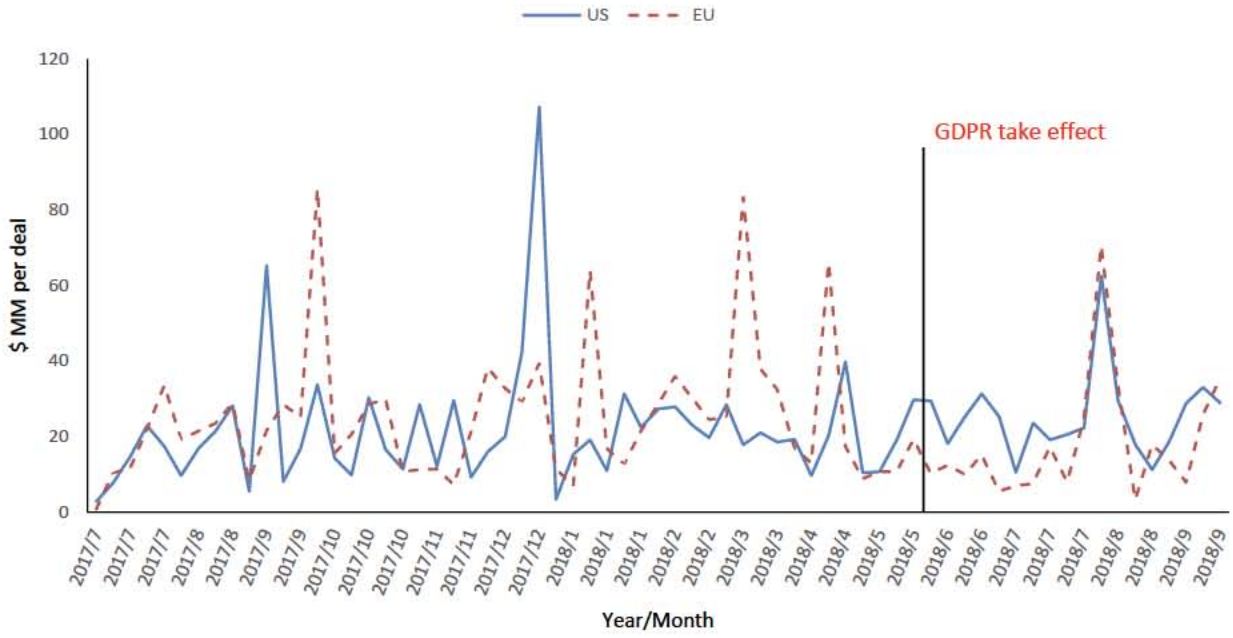


(c) Average weekly # of deals per category per state between EU and US

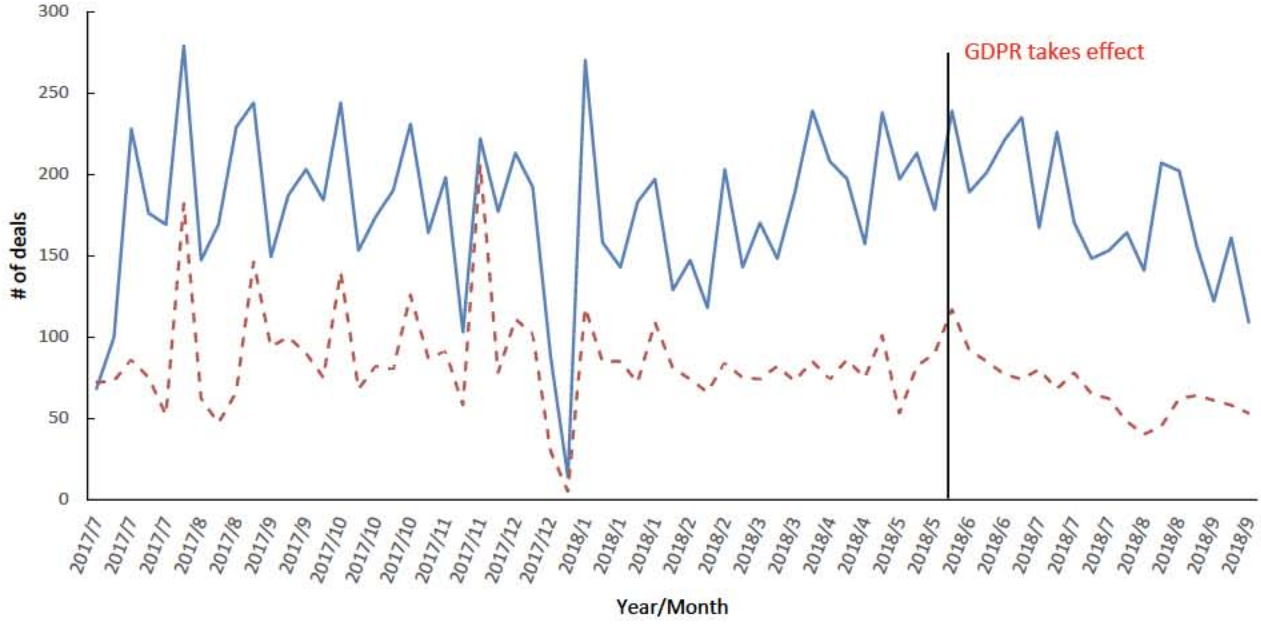


(d) Average weekly $ raised amount per category per state between EU and US

Figure1. Aggregate-level data plots

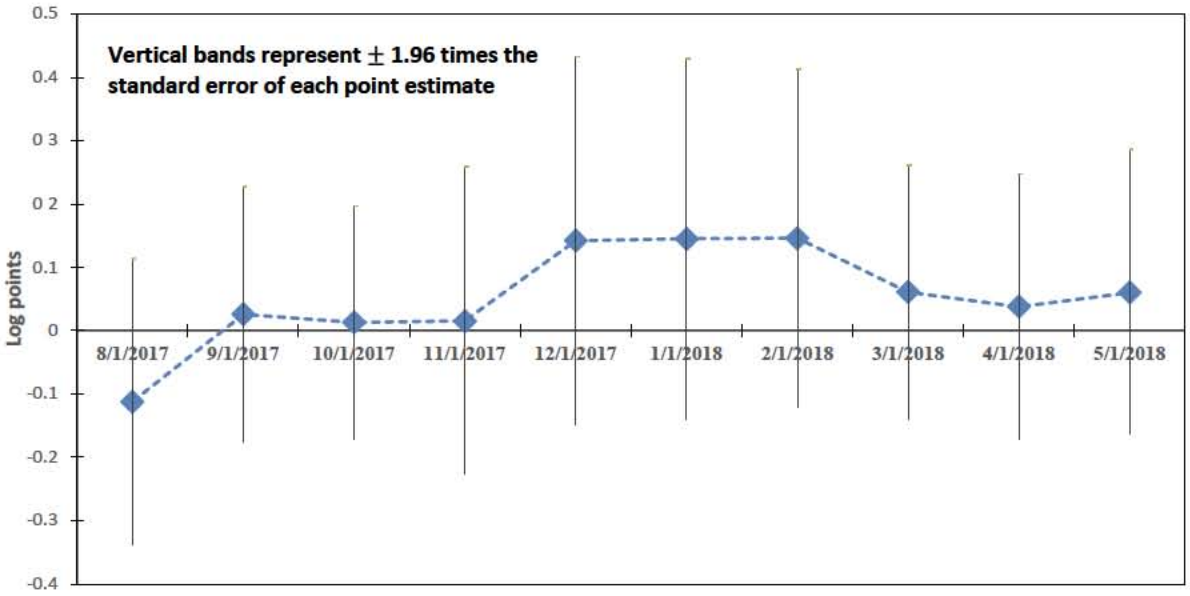


(a). Average $ amount raised per deal between EU and US

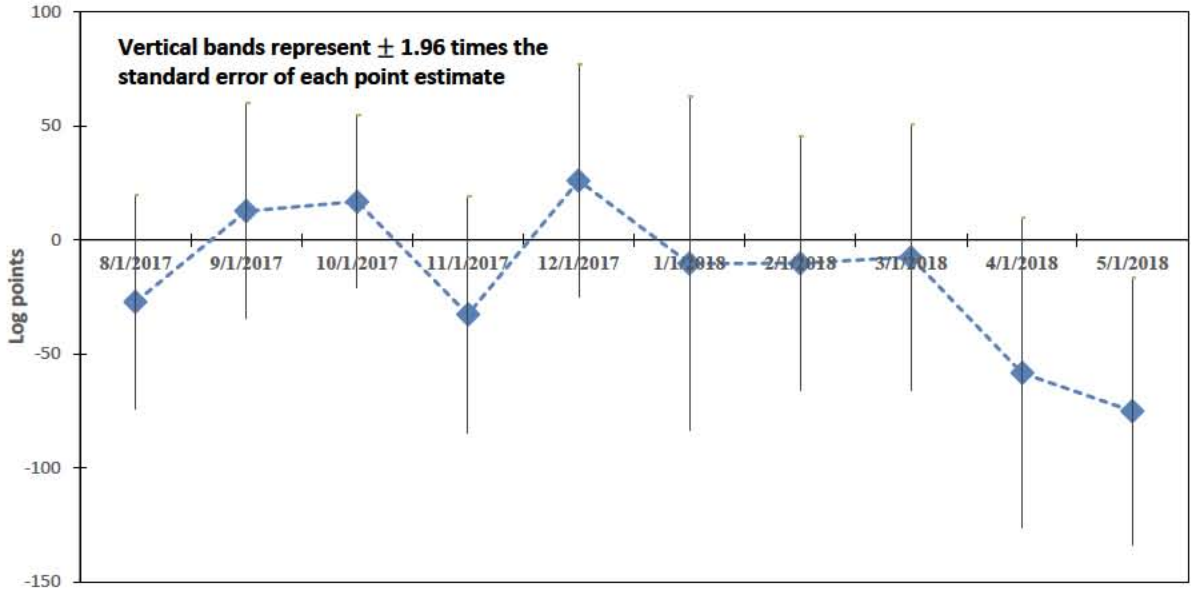


(b). Average weekly # of deals between EU and US

Figure 2. Deal-level data plots

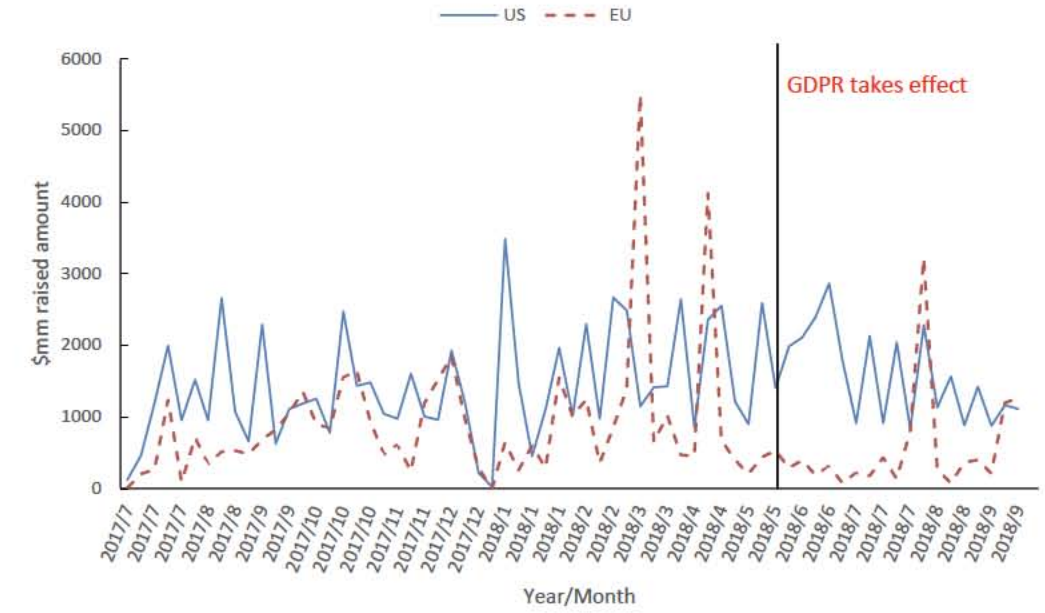


(a) Pre-treatment test for aggregate level # of deals – Poisson regression

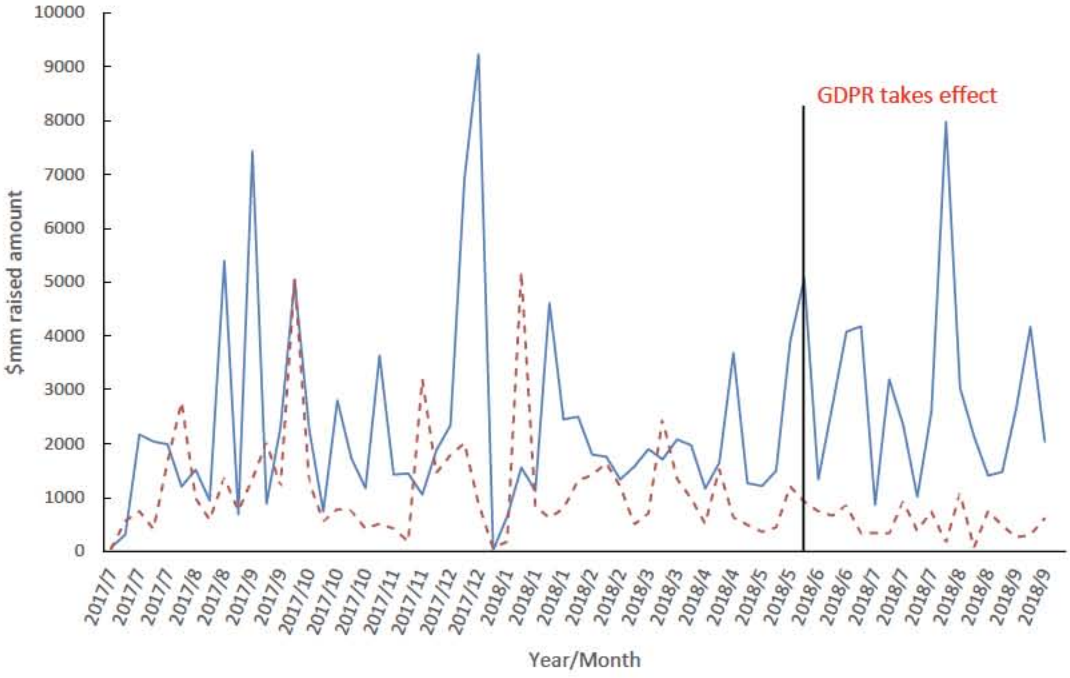


(b) Pre-treatment test for aggregate level $ raised amount – Tobit regression

Figure 3. Pre-treatment tests for aggregate level # of deals and $ raised amount

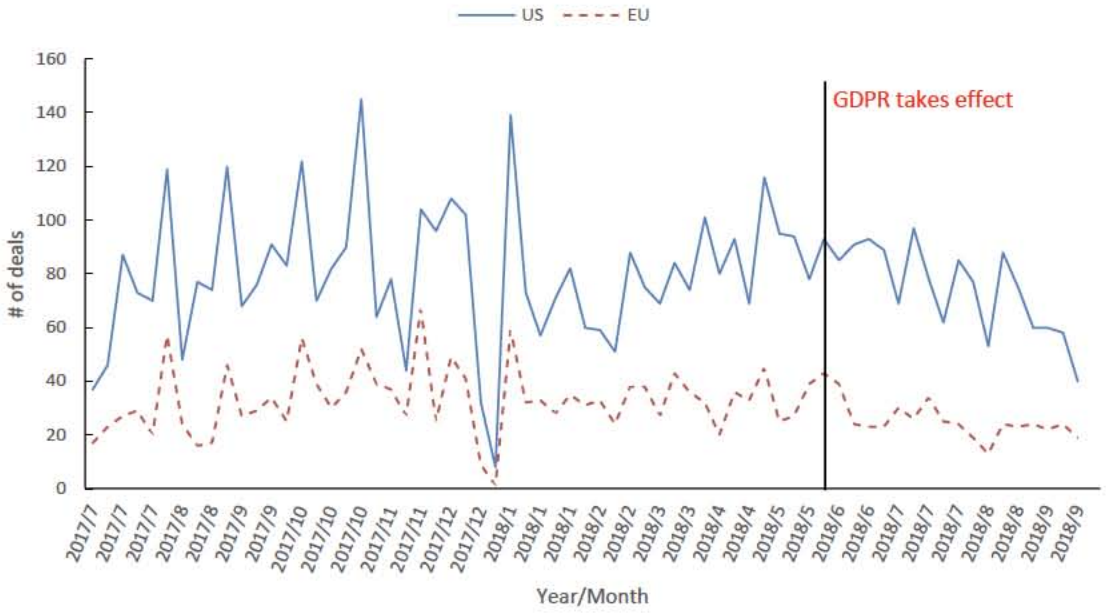


(a) Total weekly $mm raised amount – healthcare-financial category group

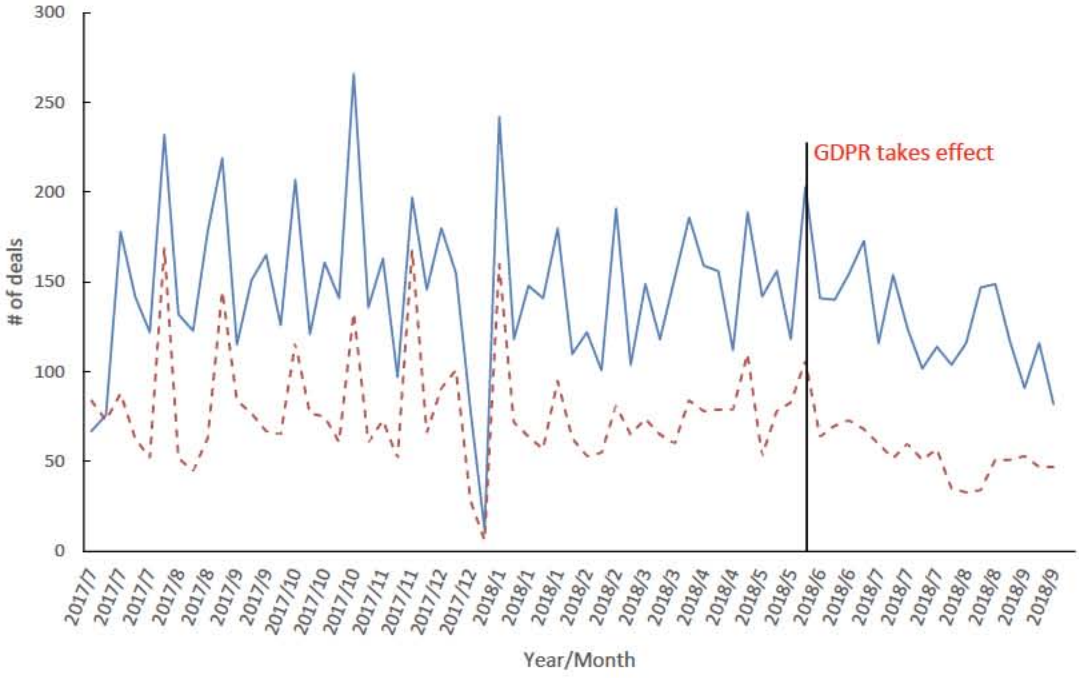


(b) Total weekly $mm raised amount – other-categories group

Figure 4. Total weekly $mm raised amount per category group



(a) Total weekly # of deals – healthcare-financial category group



(b) Total weekly # of deals – other-categories group

Figure 5. Total weekly # of deals per category group

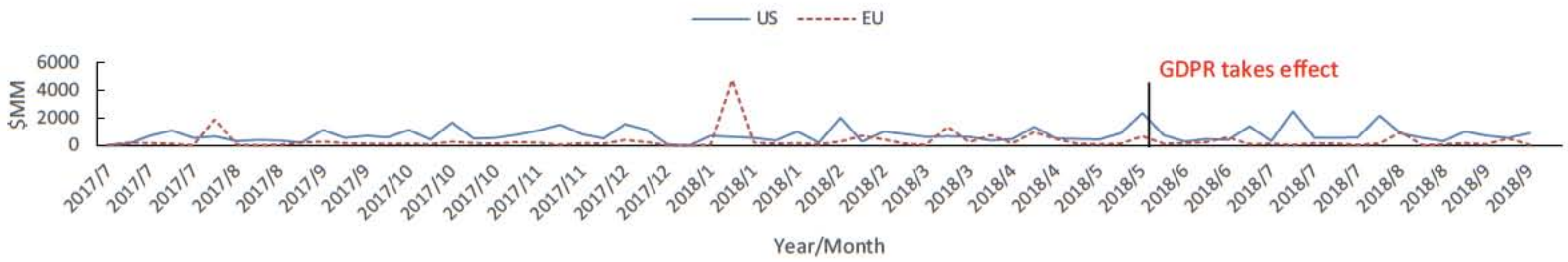
(a) New firms (0-3 year old)

(b) Young firms (3-6 year old)

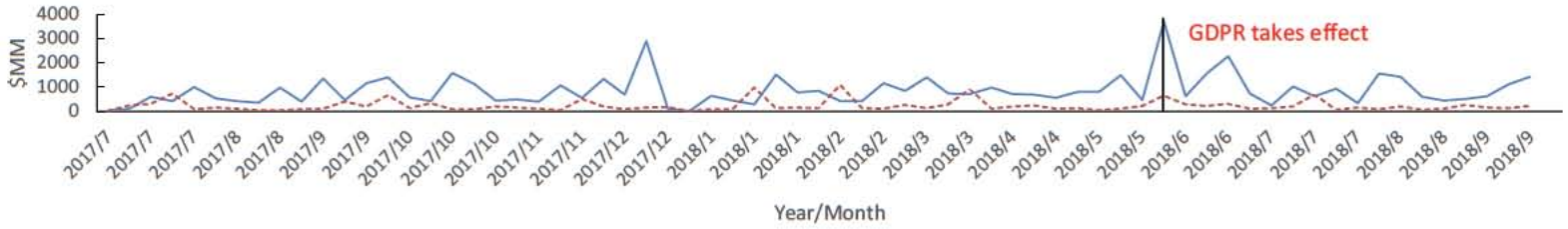
(c) Established firms (6-9 year old)

(d). Mature firms (9+ year old)

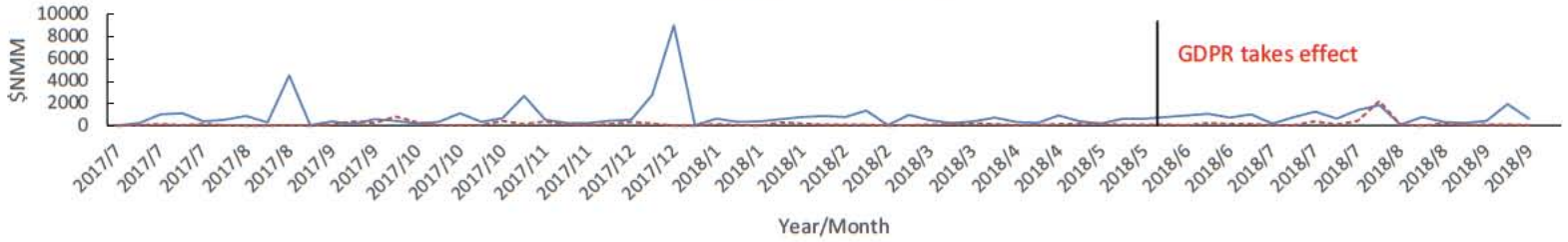
Figure 6. Weekly # of deals by firm age



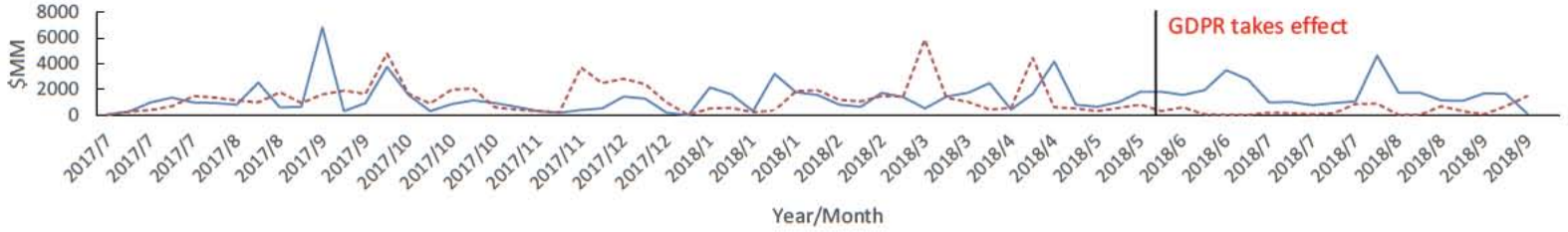
(a) New firms (0-3 year old)



(b) Young firms (3-6 year old)



(c) Established firms (6-9 year old)



(d). Mature firms (9+ year old)

Figure 7. Weekly $ amount raised by firm age

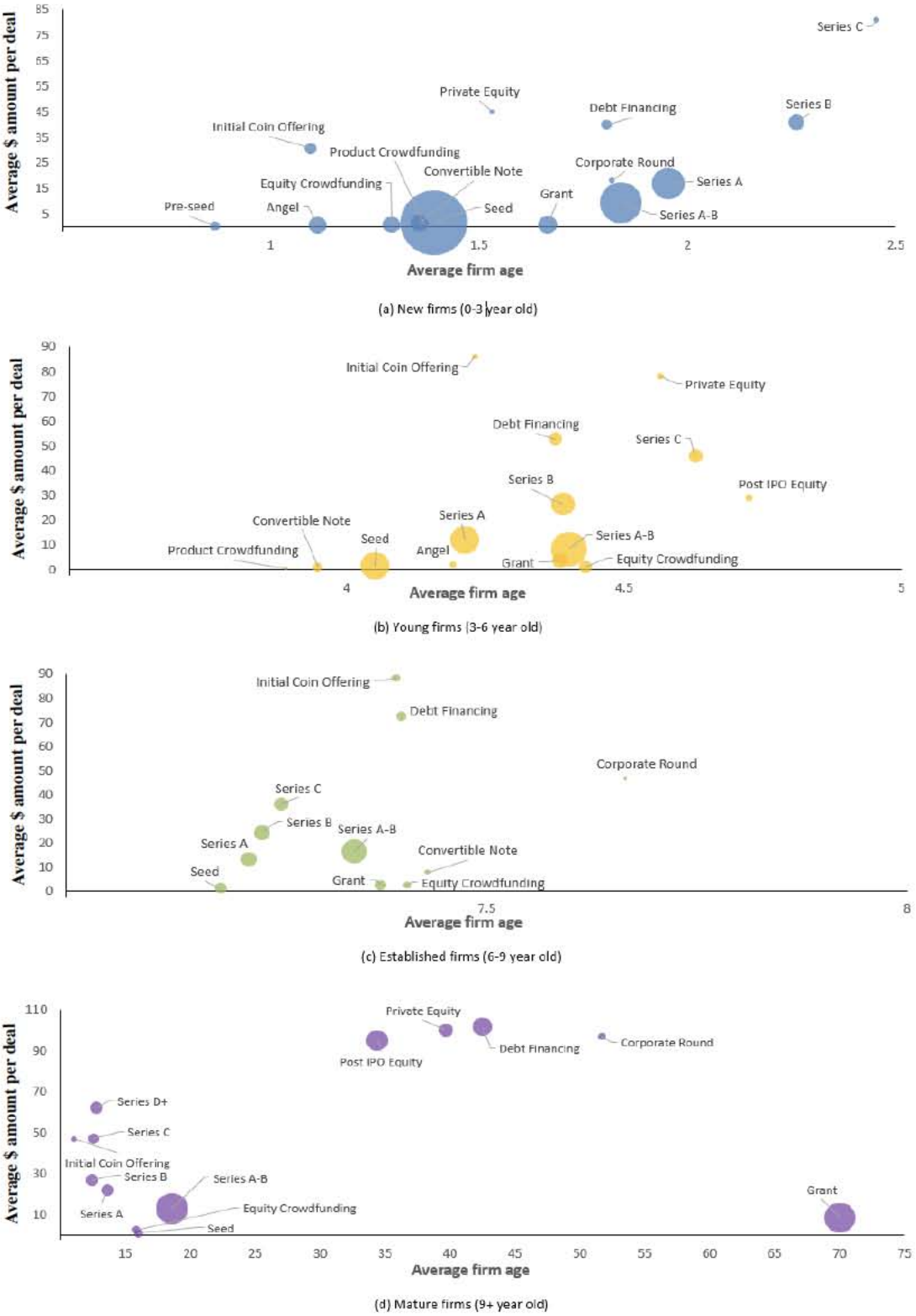


Figure 8. Funding types and size as a function of firm age (observations fewer than 10 are not depicted).

Table 1: Summary Statistics

	EU					US				
	Mean	Median	75-percentile	95-percentile	N	Mean	Median	75-percentile	95-percentile	N
Aggregate Level:										
Panel A: Whole Sample										
# of countries/states	-	-	-	-	24	-	-	-	-	51
# of weeks	-	-	-	-	67	-	-	-	-	67
# of categories	-	-	-	-	2	-	-	-	-	2
$ MM amount raised	38.04	0	3.67	174.81	3,216	38.12	0	5.14	159.82	6,834
# of deals	2.15	0	2	11	3,216	2.17	0	2	8	6,834
Unemployment	7.10%	-	-	-	-	4.00%	-	-	-	-
GDP (in billion)	298.77	-	-	-	-	398.28	-	-	-	-
CPI	109.95	-	-	-	-	114.09	-	-	-	-
Interest	-0.33%	-	-	-	-	1.56%	-	-	-	-
Panel B: Sub-group by category										
Healthcare – financial:										
$ MM amount raised	33.67	0	1.85	135.14	1,608	28.72	0	4.60	150.00	3,417
# of deals	1.29	0	1	6	1,608	1.54	0	1	7	3,417
Others:										
$ MM amount raised	42.41	0	6.52	198.22	1,608	47.52	0	5.51	38.61	3,417
# of deals	3.02	0	3	13	1,608	2.79	0	2	10	3,417
Deal Level:										
Panel C: Whole Sample										
$ MM amount raised / deal	22.27	1.42	11.69	80	5,369	21.79	3	11.22	70	11,823
Firm age (exclude mature firms)	2.94	2.56	-	-	4,544	3.05	2.67	-	-	9,620
Firm age (whole sample)	8.66	3.13	-	-	5,369	10.46	3.51	-	-	11,823
Panel D: Subgroup by category										
Healthcare-financial:										
$ MM amount raised / deal	31.76	2.36	21.99	102.39	1,692	22.09	4.2	15.51	82.00	4,379
Employee range midpoint average	705	-	-	-	1,692	464	-	-	-	4,379
Others:										
$ MM amount raised / deal	17.90	1.19	4.43	70.54	3,677	21.61	2.37	9.6	60.00	7,444
Employee range midpoint average	1049	-	-	-	3,677	909	-	-	-	7,444

Table 1 Continued

	EU					US				
	Mean	Median	75-percentile	95-percentile	N	Mean	Median	75-percentile	95-percentile	N
Panel E: Subgroup by funding stage										
Pre Stage:										
$ MM amount raised / deal	1.63	0.51	1.22	3.58	1,684	1.44	0.60	1.80	4.77	3,489
Employee range midpoint average	872	-	-	-	1,684	646	-	-	-	3,489
Main Stage:										
$ MM amount raised / deal	18.59	3	21.71	77.44	2,630	14.43	5.85	15	50	6,066
Employee range midpoint average	741	-	-	-	2,630	685	-	-	-	6,066
Late Stage:										
$ MM amount raised / deal	65.81	1.73	34.60	283.56	1,055	72.62	7.5	45	300	2,268
Employee range midpoint average	1394	-	-	-	1,055	1605	-	-	-	2,268
Panel F: Subgroup by firm age										
New firms (0-3 year):										
$ MM amount raised / deal	8.31	0.65	2.10	43.16	2,607	7.76	1.40	4.50	27	5,293
Employee range midpoint average	32	-	-	-	2,607	26	-	-	-	5,293
Young firms (3-6 year):										
$ MM amount raised / deal	17.07	2.32	17	70.86	1,415	18.82	4.20	13.32	60	3,057
Employee range midpoint average	50	-	-	-	1,415	64	-	-	-	3,057
Pre-mature firms (6-9 year):										
$ MM amount raised / deal	31.45	4	35.06	100.59	522	44.48	7.5	25	125	1,270
Employee range midpoint average	123	-	-	-	522	153	-	-	-	1,270
Mature firms (9+ year):										
$ MM amount raised / deal	69.50	7.65	50	277.23	825	46.54	6.3	25	200	2,203
Employee range midpoint average	3464	-	-	-	825	2986	-	-	-	2,203

Table 2. GDPR impact on aggregate level weekly $ raised amount

	(1)	(2)	(3)	(4)	(5)
	Dependent variable: Aggregate $MM raised amount				ln (1+$ amount)
	Baseline	Baseline with top-coded	Adding linear trend	Excluding May	OLS
postGDPR	180.955**	42.993***	44.571***	44.880***	0.977***
	(76.124)	(16.157)	(16.106)	(16.947)	(0.268)
EU_postGDPR	-54.819*	-11.574***	-11.668***	-16.659***	-0.265***
	(31.597)	(4.436)	(4.366)	(5.689)	(0.098)
Unemployment	15.936*	1.258	1.233	0.161	-0.004
	(9.242)	(1.733)	(1.683)	(1.752)	(0.031)
GDP	0.044	0.006	0.007	0.007	0.000
	(0.027)	(0.006)	(0.006)	(0.006)	(0.000)
CPI	-32.596*	-6.924*	-6.833*	-5.866	-0.108
	(17.709)	(3.962)	(4.004)	(3.908)	(0.075)
Interest rate	64.848**	26.208***	26.534***	20.557***	0.231*
	(28.565)	(6.801)	(6.910)	(7.066)	(0.123)
Effect at post GDPR mean	-13.896**	-3.380***	-3.403***	-4.488***	
	(6.695)	(1.074)	(1.054)	(1.155)	
State FE	Yes	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes	Yes
Linear Trend	No	No	Yes	No	No
Top Coded	No	Yes	Yes	Yes	No
Observations	10,050	10,050	10,050	9,300	10,050
R-squared	-	-	-	-	0.578
F-test on pre-treatment (p-value)	0.475	0.101	0.108	0.142	0.116

*Note: We group our sample into two different sub-categories (i.e., healthcare-financial, and others). The standard errors are clustered by state level (i.e., country level in EU and state level in US) in all specifications. We use 95 percentile value of $ raised amount (i.e., 175 million) as the value to top coded in Tobit regression. ***, **, and * indicate significance at the 1%, 5%, and 10% levels.*

Table 3. GDPR impact on aggregate level # of deals

	(1)	(2)	(3)	(4)
	Dependent variable: # of deals			ln (1+ # of deals)
	Baseline	Adding linear trend	Excluding May	OLS
postGDPR	-0.183	-0.248	-0.164	-0.006
	(0.190)	(0.205)	(0.194)	(0.074)
EU_postGDPR	-0.194***	-0.194***	-0.259***	-0.062*
	(0.070)	(0.068)	(0.085)	(0.033)
Unemployment	0.043	0.036	0.025	0.016
	(0.035)	(0.037)	(0.041)	(0.012)
GDP	-0.000	-0.000	-0.000	-0.000
	(0.000)	(0.000)	(0.000)	(0.000)
CPI	0.065	0.068	0.074	-0.006
	(0.064)	(0.065)	(0.062)	(0.017)
Interest rate	-0.004	-0.018	-0.043	0.089***
	(0.109)	(0.112)	(0.111)	(0.032)
State FE	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
Linear Trend	No	Yes	No	No
Observations	10,050	10,050	9,300	10,050
R-squared	-	-	-	0.733
F-test on pre-treatment (p-value)	0.585	0.582	0.670	0.117

*Note: We group our sample into two different sub-categories (i.e., healthcare – financial, and others). The standard errors are clustered by state level (i.e., country level in EU and state level in US) in all specifications. ***, **, and * indicate significance at the 1%, 5%, and 10% levels.*

Table 4 GDPR impact on $ raised amount per deal

	(1)	(2)	(3)	(4)
	Dependent variable: ln ($ amount per deal)			
	Baseline	Baseline with top-coded	Adding linear trend	Excluding May
postGDPR	-0.127	-0.103	-0.125	2.446***
	(0.285)	(0.272)	(0.284)	(0.322)
EU_postGDPR	-0.396***	-0.380***	-0.397***	-0.355***
	(0.074)	(0.071)	(0.074)	(0.087)
Firm age	0.004**	0.004***	0.004**	0.004***
	(0.001)	(0.001)	(0.001)	(0.001)
Unemployment	-0.002	-0.001	-0.007	-0.008
	(0.038)	(0.038)	(0.038)	(0.039)
GDP	0.000***	0.000***	0.000***	0.000***
	(0.000)	(0.000)	(0.000)	(0.000)
CPI	-0.359***	-0.331***	-0.358***	-0.320***
	(0.095)	(0.093)	(0.095)	(0.093)
Interest rate	0.079	0.054	0.072	0.117
	(0.119)	(0.107)	(0.120)	(0.112)
State FE	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
Linear Trend	No	No	Yes	No
Top Coded	No	Yes	No	No
Observations	17,192	17,192	17,192	15,914
R-squared	0.382	0.391	0.382	0.386

*Note: We group our sample into two different sub-categories (i.e., healthcare - financial, and others). The standard errors are clustered by state level (i.e., country level in EU and state level in US) in all specifications except for specifications. We use 95 percentile value of $ raised amount (i.e., 75 million) as the value to top coded in Tobit regression. ***, **, and * indicate significance at the 1%, 5%, and 10% levels.*

Table 5. GDPR impact on healthcare-financial and others

	(1)	(2)	(3)	(4)	(5)	(6)
	Poisson regression on # of deals		Tobit regression on total $ amount		OLS on ln ($ amount per deal)	
postGDPR	0.092	-0.270	59.561***	25.822	-0.322	-0.111
	(0.335)	(0.198)	(19.638)	(16.256)	(0.441)	(0.301)
EU_postGDPR	-0.209***	-0.186**	-22.009***	-2.934	-0.566***	-0.284***
	(0.060)	(0.090)	(5.824)	(5.597)	(0.171)	(0.080)
Unemployment	0.078	0.027	1.054	1.306	0.005***	0.005**
	(0.061)	(0.041)	(2.798)	(2.652)	(0.002)	(0.002)
GDP	-0.000	-0.000	0.011	0.003	-0.053	0.042
	(0.000)	(0.000)	(0.007)	(0.008)	(0.084)	(0.068)
CPI	0.051	0.063	-7.149	-5.743	0.000**	0.000***
	(0.080)	(0.068)	(5.051)	(3.701)	(0.000)	(0.000)
Interest rate	-0.069	0.025	8.977	38.208	-0.590***	-0.245**
	(0.158)	(0.100)	(9.218)	(8.589)	(0.144)	(0.094)
Effect at post GDPR mean			-5.216*** (0.891)			
Category	Healthcare-financial	Others	Healthcare-financial	Others	Healthcare-financial	Others
State FE	Yes	Yes	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes	Yes	Yes
Top coded	-	-	Yes	Yes	No	No
Observations	5,025	5,025	5,025	5,025	6,071	11,121
R-squared					0.410	0.372
F-test on pre-treatment (p-value)	0.100	0.985	0.102	0.302		

*Note: The standard errors are clustered by state level (i.e., country level in EU and state level in US). We also top code for each funding stage by their 95-percentile value on $ raised amount per deal, respectively. ***, **, and * indicate significance at the 1%, 5%, and 10% levels.*

Table 6. GDPR impact on total $ amount per week per state by firm age

	(1)	(2)	(3)	(4)
	Tobit regression on aggregate $ amount			
postGDPR	8.500**	13.228**	42.128***	74.527**
	(3.471)	(6.495)	(15.108)	(31.400)
EU_postGDPR	-3.204*	0.637	4.100	-58.154***
	(1.863)	(2.718)	(5.050)	(11.703)
Firm age	0.783	0.372	1.170	-1.397
	(0.482)	(1.117)	(1.074)	(3.596)
Unemployment	0.002	0.002	0.017***	-0.002
	(0.001)	(0.002)	(0.003)	(0.014)
GDP	-1.796*	0.126	-6.431**	-21.523**
	(0.942)	(2.022)	(2.691)	(8.555)
CPI	2.948	2.817	12.041**	50.506***
	(1.863)	(4.060)	(5.234)	(16.939)
Interest rate	8.500**	13.228**	42.128***	74.527**
	(3.471)	(6.495)	(15.108)	(31.400)
Effect at post	-0.902**			-7.099***
GDPR mean	(0.422)			(0.248)
Firm age group	New Firm (0-3 y.o.)	Young Firm (3-6 y.o.)	Established Firm (6-9 y.o.)	Mature Firm (9+ y.o.)
State FE	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
Top Coded	Yes	Yes	Yes	Yes
Observations	5,025	5,025	5,025	5,025
F-test on pre-treatment (p-value)	0.319	0.102	0.509	0.130

*Note: The standard errors are clustered by state level (i.e., country level in EU and state level in US). We also top code for each funding stage by their 95-percentile value on $ raised amount per deal, respectively. ***, **, and * indicate significance at the 1%, 5%, and 10% level.*

Table 7. GDPR impact on # of deals per week per state by firm age

	(1)	(2)	(3)	(4)
	Poisson regression on # of deals			
postGDPR	-0.681**	0.256	0.984*	0.732
	(0.266)	(0.317)	(0.580)	(0.540)
EU_postGDPR	-0.211**	0.022	0.047	-0.350***
	(0.087)	(0.085)	(0.188)	(0.105)
Firm age	0.004	0.115*	0.062	0.029
	(0.038)	(0.061)	(0.066)	(0.056)
Unemployment	-0.000**	-0.000	0.000	0.000
	(0.000)	(0.000)	(0.000)	(0.000)
GDP	-0.081	0.044	0.064	0.162
	(0.064)	(0.079)	(0.092)	(0.152)
CPI	0.415***	0.120	0.082	-0.100
	(0.086)	(0.125)	(0.182)	(0.229)
Interest rate	-0.681**	0.256	0.984*	0.732
	(0.266)	(0.317)	(0.580)	(0.540)
Firm age group	New Firm (0-3 y.o.)	Young Firm (3-6 y.o.)	Established Firm (6-9 y.o.)	Mature Firm (9+ y.o.)
State FE	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
Observations	5,025	5,025	5,025	5,025
F-test on pre-treatment (p-value)	0.116	0.586	0.160	0.193

*Note: The standard errors are clustered by state level (i.e., country level in EU and state level in US). We also top code for each funding stage by their 95-percentile value on $ raised amount per deal, respectively. ***, **, and * indicate significance at the 1%, 5%, and 10% level.*

Table 8. GDPR impact on $ raised per deal by firm age

	(1)	(2)	(3)	(4)
	OLS on ln ($ amount per deal)			
postGDPR	0.379	-0.420	-0.034	-1.763**
	(0.397)	(0.342)	(1.057)	(0.823)
EU_postGDPR	-0.271*	-0.314*	-0.773**	-0.436
	(0.159)	(0.176)	(0.343)	(0.284)
Firm age	0.212***	0.161***	0.012	-0.003***
	(0.027)	(0.047)	(0.051)	(0.001)
Unemployment	0.051	0.032	-0.119	-0.272*
	(0.071)	(0.135)	(0.141)	(0.159)
GDP	0.000***	-0.000	0.000***	0.000***
	(0.000)	(0.000)	(0.000)	(0.000)
CPI	-0.185*	-0.313**	-0.733**	-0.666*
	(0.095)	(0.147)	(0.344)	(0.344)
Interest rate	0.111	0.190	0.288	0.577
	(0.138)	(0.198)	(0.428)	(0.433)
Firm age group	New Firm (0-3 y.o.)	Young Firm (3-6 y.o.)	Established Firm (6-9 y.o.)	Mature Firm (9+ y.o.)
State FE	Yes	Yes	Yes	Yes
Week FE	Yes	Yes	Yes	Yes
Top Coded	No	No	No	No
Observations	7,900	4,472	1,792	3,028
R-squared	0.414	0.374	0.408	0.275

*Note: The standard errors are clustered by state level (i.e., country level in EU and state level in US). We also top code for each funding stage by their 95-percentile value on $ raised amount per deal, respectively. ***, **, and * indicate significance at the 1%, 5%, and 10% level.*

Table 9. Back-of-the-envelope estimates of a range on the job losses incurred by 0-3 year-old firms

	(1)	(2)	(3)	(4)	(5)
	Poisson Regression	OLS	Tobit Regression	Back-of-the-envelope calculations	
Variables	# of deals	$ amount per deal	Aggregate $ amount	# of deals * $ amount/deal	Aggregate $ amount
EU_postGDPR	-0.211**	-0.271*	-3.204*		
	(0.087)	(0.159)	(1.863)		
% reduction in # of deals	19.02%				
Average $mm % change per deal		27.1%			
Aggregate $mm amount change			0.902		
$mm raised/deal (post GDPR)				3.321	
# of deals (post GDPR)				690	
Aggregate $mm per week per state					14.41
Estimated total $mm reduction				1589.77	1217.70
Average firm age				1.21	1.21
Annualized $mm/employee lower bound				0.123	0.123
Annualized $mm/employee upper bound				1.020	1.020
Job loss lower bound (post GDPR)				1,559	1,194
Job loss upper bound (post GDPR)				12,899	9,880
Ratio of Jun–Sep 2017 deal activity to that in the entirety of 2017				0.331	0.331
Annualized job loss lower bound				4,705	3,604
Annualized job loss upper bound				38,931	29,819
Subsample employee # lower bound				88,092	88,092
Subsample employee # upper bound				266,352	266,352
% job loss calculation lower bound				5.34%	4.09%
% job loss calculation upper bound				14.62%	11.20%

Note: The estimates of the effects on the $ mm raised per deal, # of deals, and aggregate $mm in the post-GDPR period are used for back-of-the-envelope calculations of the effect on jobs. First, an estimate decrease in total $mm invested due to GDPR is calculated. Next, ventures founded on or after 2015 are used to calculate the average $ amount raised per employee (total $ amount raised by each firm divided by the firm's employee range). Those bounds are averaged and annualized. A job-loss range in 2018 Q3 is obtained by dividing the total $mm reduction by the annualized $mm/employee range. We extrapolate 2018 Q3 to an entire calendar year by using the ratio of deals in 2017 Q3 to 2017 in order to annualize the job loss bounds. In the final step, these bounds are given as % of the total range on the # of employees for ventures founded on or after 2015.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

(b) (6)

surveillance

1 message

(b) (6)
To: (b) (6) ,(b) (6)
Cc: (b) (6)

Thu, Oct 17, 2019 at 11:39 AM

(b) (6), (b) (6),
The two excerpts below were what got me thinking about some of the issues I mentioned yesterday. Maybe we can make a brief reference if we want to signal that this would fall within the scope of our research.

From NSA GC's NY Times piece:

"We thought wrestling with the challenges of the Fourth Amendment in addressing electronic surveillance over the past few decades was complicated and contentious, but setting norms for AI will surely be even more fraught with difficulty. The stakes are much higher, given that AI will be intrinsic to determinations and decisions of almost every aspect of our personal, professional and commercial lives. AI opens up the possibility of rendering intelligible for national security purposes that ocean of data."

https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html

Former NSA counsel article:

Historically our laws and regulations have controlled who may collect intelligence, whose communications may be collected, how they may be collected, and what may be collected. Once information about U.S. Persons has been lawfully collected, we also regulate how and to whom it may disseminated, but we have not regulated the conditions or frequency under which the collecting agency may access or analyze it. Section 702 is merely an example of this historical way of doing business. The protections afforded to U.S. Persons through collection rules always seemed sufficient to protect our liberty. I predict this is going to change. We are probably at the threshold of a new era. In the future, we are likely to be at least as concerned with the state's ability to access information already collected, or available in the marketplace, as we have been with the conditions under which the state may collect it using its own resources.

Greater attention to data access as opposed to data collection will also be impelled by a change in intelligence agencies' mission. Their task is no longer simply to acquire the communications of known foreign agents or to hunt moles in their own organizations, as was the case throughout the Cold War. Knowing who the foreign targets were was relatively easy. Stealing their communications was hard. That mission is now accompanied by a new one that has deep legal and public support, namely, to discover terrorist networks before they can wreak havoc. In the foreseeable future, this challenge will probably condition the intersection between government's intelligence gathering and citizens' rights more than any other factor, yet it strangely finds no place in this book. In pursuit of terrorists, stealing the secrets is usually the less difficult task. The harder and more important part is knowing who they are, and that involves access, under controlled conditions, to communications data in bulk – to both metadata and to lawfully collected intercepts – and sifting them for information with intelligence value. To a significant degree, therefore, the challenge in intelligence collection

has been turned on its head. Whether we like it or not, from now on more and more information will be in government hands or easily available to government. Increasingly the questions will be: When can government look at it? And how can we police abuses? [649]

http://jnslp.com/wp-content/uploads/2018/09/Review_of_The_Future_of_Foreign_Intelligence_3.pdf

The New York Times | https://nyti.ms/2A5RnMT

I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution.

Technology is about to upend our entire national security infrastructure.

By Glenn S. Gerstell
Mr. Gerstell is the general counsel of the National Security Agency.

Sept. 10, 2019

The National Security Operations Center occupies a large windowless room, bathed in blue light, on the third floor of the National Security Agency's headquarters outside of Washington. For the past 46 years, around the clock without a single interruption, a team of senior military and intelligence officials has staffed this national security nerve center.

The center's senior operations officer is surrounded by glowing high-definition monitors showing information about things like Pentagon computer networks, military and civilian air traffic in the Middle East and video feeds from drones in Afghanistan. The officer is authorized to notify the president any time of the day or night of a critical threat.

Just down a staircase outside the operations center is the Defense Special Missile and Aeronautics Center, which keeps track of missile and satellite launches by China, North Korea, Russia, Iran and other countries. If North Korea was ever to launch an intercontinental ballistic missile toward Los Angeles, those keeping watch might have half an hour or more between the time of detection to the time the missile would land at the target. At least in theory, that is enough time to alert the operations center two floors above and alert the military to shoot down the missile.

But these early-warning centers have no ability to issue a warning to the president that would stop a cyberattack that takes down a regional or national power grid or to intercept a hypersonic cruise missile launched from Russia or China. The cyberattack can be detected only upon occurrence, and the hypersonic missile, only seconds or at best minutes before attack. And even if we could detect a missile flying at low altitudes at 20 times the speed of sound, we have no way of stopping it.

The threats of cyberattack and hypersonic missiles are two examples of easily foreseeable challenges to our national security posed by rapidly developing technology. It is by no means certain that we will be able to cope with those two threats, let alone the even more complicated and unknown challenges presented by the general onrush of technology — the digital revolution or so-called Fourth Industrial Revolution — that will be our future for the next few decades.

The digital revolution has urgent and profound implications for our federal national security agencies. It is almost impossible to overstate the challenges. If anything, we run the risk of thinking too conventionally about the future. The short period of time our nation has to prepare for the effects of this revolution is already upon us, and it could not come at a more perilous and complicated time for the National Security Agency, Central Intelligence Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation and the other components of the intelligence community.

[If you're online — and, well, you are — chances are someone is using your information. We'll tell you what you can do about it. Sign up for our limited-run newsletter.]

The immediacy and specificity of the war on terror following the Sept. 11 attacks permitted the intelligence community to reorient itself relatively quickly and effectively from the Cold War and its immediate aftermath. But the intelligence community and its allies who rely on one another for information-sharing must now adapt to adversaries with new capabilities — principally China, Russia, Iran and North Korea, each of which presents different and complex threats — while still not forsaking the counterterrorism mission.

Gearing up to deal with those new adversaries, which do not necessarily present merely conventional military threats, is itself a daunting challenge and one that must be undertaken immediately and for at least the next decade or two. But that is precisely when we must put in place a new foundation for dealing with the even more profound and enduring implications of the digital revolution.

That revolution will sweep through all aspects of our society so powerfully that our only chance of effectively grappling with its consequences will lie in taking bold steps in the relatively near term. In short, our attention must turn to a far more complex set of threats of multiple dimensions enabled by the digital revolution. While the potential consequences are less catastrophic than nuclear war, they are nonetheless deeply threatening in a range of ways we will have trouble countering.

There are four key implications of this revolution that policymakers in the national security sector will need to address:

The first is that the unprecedented scale and pace of technological change will outstrip our ability to effectively adapt to it. Second, we will be in a world of ceaseless and pervasive cyberinsecurity and cyberconflict against nation-states, businesses and individuals. Third, the flood of data about human and machine activity will put such extraordinary economic and political power in the hands of the private sector that it will transform the fundamental relationship, at least in the Western world, between government and the private sector. Finally, and perhaps most ominously, the digital revolution has the potential for a pernicious effect on the very legitimacy and thus stability of our governmental and societal structures.

What I offer here is more of a sketch than a finished painting; our national policymakers and the future leaders of those agencies will be responsible for addressing these foreseeable challenges and ultimately finding solutions. While these trends have been extensively discussed in the press, academia and the technical world, there has been far less attention devoted to understanding the combined effect the trends will have on the various agencies that help keep our nation safe. I hope to rectify that shortfall.

We all sense that we are on the cusp of unimaginable technological changes. Cellphones and the internet seem of such manifest utility that we take them for granted, but that is only because they have become so central to our daily lives, not because they have been around forever. Indeed, as we are often reminded, Google started in 1998. YouTube is only 14 years old, and the iPhone is merely 12 years old. The digital revolution thus far is distinguished by its ability to become ubiquitous in our daily personal and commercial lives in an astonishingly rapid time, a time frame that is really without precedent.

Other transformational technologies, such as railroads, electricity, radio, television, automobiles and airplanes, all took several decades before they reached that comparable level of ubiquity. Society had the time to sort out the norms, rules and laws governing those technologies and the respective roles of government and the private sector. Consider, for example, the lag between the advent of the first useful automobile in the late 19th century and the late 1960s, when safety features became truly significant and mandatory. By contrast, today, just a dozen years after Facebook became a “thing” in our lives, we are forced to grapple with whether and how we should regulate hateful postings and mendacious foreign electoral influence on social media platforms.

Facial recognition technology has in just a handful of years become sufficiently accurate as to be useful and thus more common, but its persistent imperfections have led to a confused spate of lawsuits and statutes seeking to regulate its use. We are far from figuring out its proper role in our society. So the windows for how long it takes for technology to shape society and — more pertinent to this discussion — how long it takes for us to sort out the associated challenges are becoming almost impossibly compressed.

The time compression for our society and ultimately our national security agencies to deal with these challenges is but one aspect of the problem. The sheer amount of data that will be generated by individual and commercial activities, with the Internet of Things and 5G cellular connectivity, is incomprehensible and will require entirely new ways of rendering that data meaningful to agencies whose mission is to discern threats to national security.

We will need new technologies and systems to capture, analyze and store this data. Obviously, that will require enormous investments by the United States and its allies to upgrade national security and surveillance systems. Will Western liberal democracies, already straining under the combined demands of decaying civil infrastructure, aging populations, upgrading militaries and so on, be able to afford these investments? Given that there is no specific forcing event to require greater resources, but rather a trend, history suggests that we will appreciate the seriousness of the underinvestment only when a crisis has occurred.

That approach might be a barely acceptable way for our society and government to address social ills and decaying infrastructure, which are slower-moving problems, where with enough resources one might catch up. But the same approach could well be disastrous when addressing rapidly evolving technological matters, especially where national security is at stake. Without such investments, our national security agencies risk becoming profoundly less effective or marginalized.

While extraordinary levels of new investment will be required to deal with the sheer quantity of data, that alone will not be sufficient. It is futile to believe that we will be able to spend our way to success. Rather, we will need to couple large investment with entirely new ways of approaching how we collect, manage and make sense of this data. One key aspect of any such new approach will be a heavy reliance on machine learning and artificial intelligence. We thought wrestling with the challenges of the Fourth Amendment in addressing electronic surveillance over the past few decades was complicated and contentious, but setting norms for A.I. will surely be even more fraught with difficulty. The stakes are much higher, given that A.I. will be intrinsic to determinations and decisions of almost every aspect of our personal, professional and commercial lives. A.I. opens up the possibility of rendering intelligible for national security purposes that ocean of data. But if misused or even if not thoroughly understood, A.I. can yield nefarious and corrupting results for our society.

Since A.I. is still relatively nascent, our surveillance and analytic resources are not well positioned to deeply understand how adversaries might be using it in the future. The range of novel issues is daunting. For example, we will need to understand how to defend our analytic systems against data poisoning, in which an adversary can feed misinformation to A.I. systems to corrupt or

defeat them (such as causing a driverless car to ignore a stop sign).

We will also need to understand the protocols by which future autonomous weapons — drones, tanks, armed robots — will be controlled so that we can defend ourselves. Will the availability of huge numbers of nonhuman war-fighting machines increase the chances of war, as policymakers might be more willing to sacrifice those machines than humans? Or will such machines permit some not-yet-conceived lower threshold of machine-to-machine conflict — whether involving cyber or physical machines — that does not rise to the level of a full-fledged war? Our national security agencies will require new experts and resources to understand the intentions and capabilities of adversaries in this new and developing area.

Understanding the promise and threat of quantum computing will also require vast expansion of our expertise in this extraordinarily sophisticated area. It is true that no one has yet built a functioning quantum computer. Perhaps no one ever will. But it seems more likely than not that before the middle of this century either China or the United States will do so, with extraordinary advantages for whichever nation gets there first.

Unlike the electronic digital computers we have used for over a half century, quantum computers are based on a fundamentally different concept, relying not on simple “on” and “off” states of electricity but on the complex properties of atomic and subatomic particles. One strategic benefit is that quantum computing will enable something that even our current supercomputers cannot do — crack strong encryption of the type that now protects our commercial financial transactions, our weapons systems and government’s secret communications. China’s publicly announced 2030 goal is to develop a high-performing quantum computer, which should have that decryption ability. Imagine the havoc that could create. Imagine the overwhelming leverage that the winner would have — such a decryption ability could render the military capabilities of the loser almost irrelevant and its economy overturned.

The analogy of the postwar world in which there was only one nuclear power hints at the type of unilateral dominance that might be possible for the quantum computing victor — but it is not apt here. Even with a nuclear monopoly, there were very real limits on utilizing that capability. But not so with the unilateral capability to decrypt — and thus to understand and perhaps to interfere with or destroy — the entire digital existence of an adversary country.

The strategic advantage here would be for one country to surreptitiously acquire such a capability and maintain it for perhaps several years or more. Other countries would not realize that everything from their weapons systems to financial transactions would be vulnerable during that period; and that would include not only current activity but also the historic, encrypted communications collected and retained by the winner in anticipation of this very capability.

Indeed, one of the strategies yet to be developed involves the paradox of how a country with such capability could exploit it without revealing the capability’s existence. Moreover, shifting to quantum-resistant algorithms and encryption is theoretical and thus uncertain, but will surely be expensive and a decades-long endeavor.

Over the past several decades, the intelligence community has built up an extraordinary capability to understand the military doctrines and weapons systems of Russia and China. That will still be relevant, but there is now a fundamentally new additional requirement. Under the best of circumstances, it would take many years to develop comparable levels of expertise about those countries’ use of A.I., quantum computing or other novel technologies. Such technologies range from hypersonic missiles, which Russia and China are racing to develop — with the potential to upend the entire global balance of power — to synthetic biology and genetic manipulation, with the potential to create new biological weapons or immunities. Our national security sector does not have an extensive history of marrying intelligence insight and analysis with deep technical expertise across a wide range of scientific disciplines.

That might not, however, be the limiting factor.

It is by no means assured that our national security sector will be able to attract on a sufficient scale the scarce engineering, mathematical and scientific talent that would supply the necessary expertise. That challenge will require investment, enlightened strategic management and an innovative approach to luring a different type of expert out of the private sector into government. Meeting this challenge will require a greater reliance in general on the private sector, since government alone does not possess the requisite expertise. A large portion of the intelligence community’s experts on the military capabilities and plans of Russia and China joined government during the Reagan administration; other experts on counterterrorism and new technology burnished their technical skills following the Sept. 11 attacks. Many of those experts are nearing retirement or have already left to join an attractive private sector. With millennials believing that technology in the private sector now allows them to help change the world — previously the idea of a mission had been largely the province of public service — it is not clear that the intelligence community will be able to attract and retain the necessary talent needed to make sense of how our adversaries will make use of the new technology.

In short, while important work has been done in examining and laying the foundations for the critical role new technologies will play in national security, much more needs to be done. We must ask whether our defense and national security establishments are in a position — financial and technical — to succeed in these critical technologies that could either solidify our continued position as the

leading global power or reduce us to a clearly subordinate role. We are talking about national initiatives that collectively will dwarf the effort to put a man on the moon.

Bluntly put, there are few signs that our society overall and our political leaders have fully embraced the challenge or appreciate the risks of failure.

All of this technological innovation will surely bring significant societal benefits, perhaps most notably in the area of health care and genetic engineering, but it will also increase — to use a hackneyed but useful term — the "attack surface" for cyber mischief. This takes us to the second implication of the digital revolution: We must prepare for a world of incessant, relentless and omnipresent cyberconflict — in not only our national security and defense systems (where we are already used to that conflict) but also, more significantly, every aspect of our daily and commercial lives.

The sensors, systems, networks, algorithms and machines that will empower our new lives — whether health care implants, driverless cars, pilotless aircraft or food safety protections — will all be part of the Internet of Things. One consequence is that the current division between cyberdefense (think firewalls, penetration testing and cyberhygiene) and supply-chain risk management (think of the assessment of equipment manufacturing, component assurance and availability and surveillance concerns in equipment) will be eliminated, with everyone concerned with the holistic sanctity of equipment and software to achieve the well-recognized triad of availability, security and integrity.

The 40-odd nation-states that today have offensive cybercapabilities will seem a quaint historic artifact when sophisticated tools for cybermischief are in the hands of not only every nation-state but also common criminals around the globe. While most nation-states might be careful to limit their cybereffects to economic theft and espionage, pre-battle positioning of beacons and other malware, mischievous interference with elections and public opinion — all below levels that cause significant physical damage to infrastructure or physical harm to humans, and thus below at least what we currently think of as the threshold for an act of war — there is no guarantee that all nations will exercise such care nor that criminals would be deterred. Consider how North Korea seems able to operate with relative impunity in cyberspace, knowing that it is unlikely to provoke an armed attack partly because of its perceived willingness to retaliate in ways that would impose unacceptable consequences on Western society. Multiply that dynamic across a dozen or more countries or international terrorists or criminal gangs and we are now faced with an entirely different national security threat.

To be sure, our nation has set forth its cyberstrategies and continues to refine its offensive and defensive doctrines in cyberspace, but nearly every expert would concede more needs to be done. The question is whether we will be able to do it in time, since the threat is coming at us with the speed and force of a tsunami.

The simple fact of the matter is that no nation has yet devised an effective solution to the conundrum of how to respond in a definitive and dispositive way to another nation-state's malicious cyberactivity. Whole-of-government approaches — economic sanctions, judicial prosecutions and offensive cyberresponse below the war threshold — while essential and appropriate, have not been enough to stop cybermalevolence. In short, the problem is going to get worse before it gets better.

In all probability, it will get better not because we develop more effective deterrents (although threats of cyberretaliation and imposition of other burdens clearly do play a key role here, at least with other nation-states) but because we develop greater resilience and more impervious defenses — and the full realization of that may be a decade away.

In the meantime, our national security agencies will be confronted with the political imperatives in our democracies of responding (at least in some way) to cyberthreats. Among other things, our citizens and businesses will have to accept that cybermalevolence is a persistent threat, not a war to be won or a disease to be cured. Moreover, since the threat is ignorant of sovereign boundaries, agencies charged with cyberprotection will be required to work with many others around the globe, perhaps including those of adversary or competitor nations, creating new complexities.

At a minimum, the worldwide cyberthreat will put a premium on trusted relations among the Five Eyes (the United States, Britain, Canada, Australia and New Zealand) and other like-minded nations, to facilitate working together to counteract malevolent activity that can span the globe in seconds. Even among such long-term, cohesive arrangements as the Five Eyes alliance, unity of effort in cyberspace is not assured, as witnessed recently by differing approaches to the risks posed by Huawei equipment in 5G networks.

The third implication of the digital revolution is that the balance between government and the private sector will be altered in a profound way. That in turn is the inescapable product of three factors: cybervulnerability affecting every element of the private sector (no longer are targets arguably limited to military assets), the general flood of data unleashed by the digital revolution that will be

created in the hands of private enterprise and a response to a rising China whose strategic technology goals pose a unique threat that directly implicates the private sector.

Even without considering the challenges presented by China, there are at least two, related manifestations of how the government-private sector balance has changed and will change. First, the government no longer possesses the lead in complex technology, at least in many areas relevant to national security. Arguably, the most powerful computing and sophisticated algorithm development now occurs not in the Pentagon or the N.S.A. but in university research labs and in the Googles and Amazons of the commercial world. (To be sure, the government still maintains its superiority in important areas ranging from nuclear energy to cryptography.) Even apart from the issue of which sector has the technological edge, there is the simple fact that the digital revolution has brought astonishing capabilities to anyone who has a smartphone, who can now download a facial recognition app, a malicious cybertool or some other capability that formerly was the exclusive province of government.

Second, the private sector will have many more times the quantity of data about individuals and commercial activity than governments could ever obtain. The larger antivirus vendors, with their sensors connected to their global corporate clients, already know more at any given moment about the state of networks around the world than does any government agency. Businesses in the services, retailing, industrial and other sectors will have more global sensors and applications detecting cybertraffic, collecting behavioral patterns, amassing personal data and so on, than even the most surveillance-oriented nation could ever hope to have. The fact that private satellite imagery companies have displaced the monopoly that the National Geospatial-Intelligence Agency used to have is merely a harbinger of how the private sector will be the collector and repository of key information about our locations, our consumption patterns, our communications — in short, about everything.

As the owners of physical infrastructure learned following the Sept. 11 terrorist attacks, when our everyday lives rely on the security of assets and services held in the private sector, commercial owners will be expected to take steps to protect society. We are clearly witnessing the same imbuing of social responsibility into how the digital revolution's data will be handled. Personal data needs to be safeguarded so that it does not fall into the wrong hands, it needs to be made accurate so that incorrect results are not generated from its use, and it needs to be used in ways that do not violate our notions of privacy and proper use. Those are not duties originating within the commercial world but will be increasingly imposed by society.

As for the safeguarding, many would argue that governments cannot and should not be relied on to prevent and defend against every cyberthreat to the private sector, even from a nation-state; such threats are not the same as an armed attack. But that leaves the private sector frustrated and underdefended — hacking back is often impossible and generally illegal.

National security agencies will need to defuse that frustration and find an effective path for collaboration with the private sector to mitigate cyberthreats. The only practical solution is for the private sector to assume a greater burden in this area, but with the active support of the national security agencies. We are still struggling to find an effective solution to the competing desires for the private sector to obtain classified information about cyberthreats and for government to obtain detailed information about cyberintrusions into corporate networks. Both sides have legitimate reasons to keep their information secret. But ultimately we all realize that will not yield an effective outcome. Attribution solutions will require the private sector to be more forthcoming about network breaches. Indeed, the private sector should have a greater responsibility to collect, analyze and retain all this new data and to make it available with appropriate safeguards to the government for national security purposes. But even safeguards will not completely allay a variety of privacy and liability concerns.

Until recently, at least in the United States, our notions of privacy have been rooted in the Fourth Amendment's delineation of the federal government's powers vis-à-vis the individual citizen. But what do our notions of privacy mean anymore when Amazon, Google, Apple, Microsoft, Facebook and so on already know so much about you? We now see increasing pressure in Congress to regulate in this area. To be sure, this article is not advocating any particular approach (much less suggesting greater surveillance powers), but it is hard to escape the conclusion that we will need to recalibrate the balance in this area of data privacy between the government and the private sector.

National security agencies should affirmatively contribute to the public discourse about this recalibration. The challenge for those agencies will be to find the right approach to working with the private sector to obtain the data needed to fulfill their vital missions in a manner that fits our values and cultures.

Of course, there is another path, and it is the one taken by authoritarian regimes around the world. China's approach is to have all that data reside in the central government, in a vast databank of personally identifying information about its citizens, from iris and facial recognition to DNA data. That is antithetical to our values.

But it is equally true that to keep our society safe, those charged with that mission will need some access to that data. Absent some satisfactory calibration, our national security agencies run the risk of being marginalized and ultimately irrelevant and ineffectual, with grave consequences for national security.

Eschewing the approach taken by authoritarian regimes to data collection and usage by no means reveals the proper path to be taken, as any decision would be deeply linked to the historic roles of government and the private sector in each country. The approach in Western Europe, with close cooperation between public and private sectors, might seem inappropriate if not impossible in America.

For two examples, consider the integrated cybercenters in Britain and the level of government involvement in private sector data usage under the European Union's General Data Protection Regulation. Would the American business community accept that model, and would our national politics permit its adoption? Paradoxically, the global cyberthreat and the overall challenges presented by the digital revolution may propel national security agencies of many countries to work together, but they may find closer cooperation difficult in practice as the balance between public and private sectors will vary greatly from nation to nation.

Finally, our nation will have no choice but to harness the collective capabilities of the government and the private sector to address the combined technologic and economic threats posed by China. For the first time since the United States became a global power, it must now confront an adversary that presents not merely a political or military threat but also an existential economic one. But in the latter area, the playing field is not level, as China advances its national strategic goals through a unified effort harnessing its government and its business sectors (the latter being a mix of private and state-sponsored endeavors) — while our strategic goals are seen as the responsibility of the federal government, with our private sector largely free to pursue its capitalist interests as it sees fit.

The almost inescapable fact that China's economy will surpass ours in size has obvious national security implications. But two circumstances present special challenges for our national security community. The obvious one is that China continues to seek economic and military superiority through cybertheft from our government, defense industrial base and academia. The second is that our national security agencies for the first time must amass the talent and systems to understand not simply a military challenge but also challenges across a broad range of technology and global finance issues. The capacity for such understanding currently resides principally in the private sector and our universities, not the federal government.

Both of those circumstances will force the government and private sector to work together in unprecedented coordinated and mutually supportive ways if we are to rise to the challenges posed by China. That will require changes in not only attitudes (on both sides) but also laws to permit greater collaboration.

The digital revolution is at least partly responsible for another disruptive effect on the relationship between governments and the private sector, namely the almost complete globalization of economic forces. That capital is now a global commodity shows the relative shortcomings of a nationalistic approach to protect vital assets. Most Western democracies have some rules to regulate foreign investment in critical industrial sectors. In the United States, the Chinese have figured out that it is easy to sidestep the strictures of the Committee on Foreign Investment in the United States, which limits foreign investment in nationally sensitive industries, simply by investing in start-ups and other ventures that have access or insight into critical technologies or by working in university research labs to the same end. This may well be another factor weakening the role of nation-states in providing security and tilting the balance of power toward the private sector, which is in a better position to police unwanted investments and intellectual property theft.

As if all this is not disconcerting enough, the fourth implication is that the internet can have a pernicious effect on our democracies, where adversaries can take advantage of our freedoms and interfere with our societal and government institutions. The painfully obvious fact is that the internet affords everyone a communications capability. In the absence of a commonly accepted authority — whether it be a trusted government or a curated news source — the internet permits lies and evil to be spread with almost no check.

A world in which effective deception in almost every venue and media outlet is possible vastly complicates the duties of government and societal institutions. Even if a nation were to control its own citizens' activities, information (whether accurate or not) knows no national boundaries.

We all recognize this decentralizing and delegitimizing force, and there is no need to elaborate on it here. Worth appreciating in this context, however, is that governmental agencies with a national security mission are going to find it vastly more difficult to maintain the necessary trust, respect and support of a democratic populace in this environment — jeopardizing not only their ability to obtain resources from society but also in the end their very mission.

Indeed, the state of affairs of fundamental uncertainty and doubt that will be facilitated by the misuse of digital technology may well make it more difficult to maintain foreign alliances (which, after all, are based on trust) — precisely at a time, paradoxically, when global cooperation is required to counter malicious activity. In short, and perhaps most critical to appreciate, the fourth implication of the digital revolution is that it will make dealing with the first three implications all the more problematic.

Putting these four implications together — coping with unprecedented technological change, adapting to a world of unceasing cyberconflict, navigating concepts of privacy and the power that comes with access to big data in the hands of the private sector, and countering the insidious and pernicious effects of the delegitimization afforded by the malign use of the internet — yields at least two imperatives, both of which are transformational.

The first imperative is that our national security agencies must quickly accept this forthcoming reality and embrace the need for significant changes to address these challenges. This will have to be done in short order, since the digital revolution's pace will soon outstrip our ability to deal with it, and it will have to be done at a time when our national security agencies are confronted with complex new geopolitical threats.

Much of what needs to be done is easy to see — developing the requisite new technologies and attracting and retaining the expertise needed for that forthcoming reality. What is difficult is executing the solution to those challenges, most notably including whether our nation has the resources and political will to effect that solution. The roughly $60 billion our nation spends annually on the intelligence community might have to be significantly increased during a time of intense competition over the federal budget. Even if the amount is indeed so increased, spending additional vast sums to meet the challenges in an effective way will be a daunting undertaking. Fortunately, the same digital revolution that presents these novel challenges also sometimes provides the new tools (A.I., for example) to deal with them.

The second imperative is we must adapt to the unavoidable conclusion that the fundamental relationship between government and the private sector will be greatly altered. The national security agencies must have a vital role in reshaping that balance if they are to succeed in their mission to protect our democracy and keep our citizens safe. While there will be good reasons to increase the resources devoted to the intelligence community, other factors will suggest that an increasing portion of the mission should be handled by the private sector. In short, addressing the challenges will not necessarily mean that the national security sector will become massively large, with the associated risks of inefficiency, insufficient coordination and excessively intrusive surveillance and data retention.

A smarter approach would be to recognize that as the capabilities of the private sector increase, the scope of activities of the national security agencies could become significantly more focused, undertaking only those activities in which government either has a recognized advantage or must be the only actor. A greater burden would then be borne by the private sector.

For example, our society could consider greater coordination between government and the private sector in advancing national security strategic goals (such as development of quantum computing capabilities), specific requirements for the private sector to share (with appropriate safeguards) proprietary data and technology with the government where directly relevant to national security, or a duty to notify government of the details of cyberincidents. Perhaps we should rekindle the discussion over a national service obligation to help supply technical expertise to the government across a broad range of fields, or otherwise create some arrangement to make such expertise available to government (rather than the current model in which the private sector often lures away government-trained talent). The point here is not to advocate for any of these, simply to say our policymakers need to be examining alternatives if we are to close the forthcoming technology gap.

Although I have sketched out some of the more troublesome implications of the digital revolution for the national security sector, it is not in the spirit of forecasting doom, but rather to sound an alarm.

Our innovative and entrepreneurial society affords us a unique advantage in dealing with those implications. Moreover, no adversary should ever underestimate the extraordinary capabilities of our armed forces and intelligence community — like those keeping watch at the National Security Operations Center. Their prowess and resilience will be key in addressing future challenges. But it would be a mistake to rely on these strengths alone.

Surmounting the transformational challenges posed by this Fourth Industrial Revolution will require not merely resources and creativity from both the public and private sectors but also, and more critically, a level of concerted national political will that may be made all the more difficult to achieve by the very attributes of the digital revolution rushing toward us.

Mr. Gerstell is the general counsel of the National Security Agency and previously served as a member of the president's National Infrastructure Advisory Council.

BOOK REVIEWS

A Review of "The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age" by Laura K. Donohue

Joel Brenner*

Professor Donohue has given us a full-throated denunciation of the entire legal framework regulating the government's collection of data about American citizens and permanent residents, whom we call "United States Persons."[1] She contends that in the wake of the digital revolution, current law "is no longer sufficient to guard our rights"[2] – she's right about that – and that we have actually returned to the untrammeled issuance of general warrants that characterized the eighteenth century British practice that our nation's Founders rebelled against. She proposes a thorough revision of the laws governing the collection of foreign electronic intelligence within the United States and abroad, and she advocates severe limitations on the collection and access to digital information of any sort. I will address the merits of her arguments – but first a threshold question: Is this really a book about the future of foreign intelligence?

From the half-century leading to the end of the Cold War, the nearly exclusive control by nation-states over the tools of spy craft seemed like a natural monopoly. The complexity of modern cryptography from the 1930s onward put high-end encryption beyond the capability of all but a few intelligence services.[3] Most forms of electronic intelligence gathering – advanced listening devices, sophisticated radars and antennae, and measurement of weaponry signatures, for example – were also developed by governments and were unavailable to most nations. Free-lance and commercial human spying never went away, but they became the exception after Europe was rigidly divided into East-West blocs, and as border controls, which hardly existed before World War I,[4] became the norm.

Governments' monopoly over most of the tools of spycraft did not disappear overnight. Between the collapse of the Soviet Union in 1991 and the 9/11 attacks a decade later, however, the monopoly largely vanished as these tools became the

* Joel Brenner is a senior research fellow at the Massachusetts Institute of Technology. He is the former inspector general and senior counsel of the National Security Agency and former head of U.S. counterintelligence under the first three directors of national intelligence. He gratefully acknowledges the assistance of Alexander Loomis of Harvard Law School.

1. 50 U.S.C. § 1801(i) (2012).
2. LAURA K. DONOHUE, FUTURE OF FOREIGN INTELLIGENCE 3 (2016).
3. *See generally* DAVID KAHN, THE CODE BREAKERS: THE STORY OF SECRET WRITING (1967).
4. *See History of Passports*, GOVERNMENT OF CANADA, http://www.cic.gc.ca/english/games/teachers-corner/history-passports.asp. For a colorful evocation of the period, see EVELYN WAUGH, WHEN THE GOING WAS GOOD 7-10 (1946).

products and instruments of the marketplace. The encryption now found in an ordinary smart phone can be broken only with extraordinary effort, if at all, and its computing power dwarfs anything available to the presidents and premiers of a previous generation. The monopoly of the two Cold War superpowers over high-thrust rocketry and orbital satellites is ancient history. Countries around the world now compete with, or rely on, private companies to do the heavy lifting. The commercial satellite imagery readily available to the public is also jaw-droppingly good, at resolutions that were state secrets only a few years ago. The advantage of states over private enterprises in surveillance, counter-surveillance, and clandestine operations has not disappeared, but the private sector is catching up fast. At the same time, the digitization of information and the consequent explosion of freely available data have both delighted and disoriented us, turning private lives inside out and making secrets difficult to keep for individuals, businesses, and governments alike – including intelligence services. The ubiquity of data has also made open-source intelligence more valuable than ever and has called into question the scope, though not the necessity, of secret intelligence gathering and analysis. Given advances in the application of artificial intelligence, the pace of change is not slowing down. The challenges this environment presents to intelligence services are severe.[5] In the wake of these developments, the distinction insisted upon by the grand viziers of Langley, South Bank Legoland, and Moscow Center between *i*ntelligence (that's what *you* think, with a small "i") and *I*ntelligence (that's what *we* think, with its reifying initial capital) appears risible.

Profound political, ethical, and legal challenges also confront agencies that make a living stealing secrets. Stealing secrets involves breaking the laws of other nations, including friendly ones. In an increasingly integrated world, we can expect new norms, and perhaps laws, to control that kind of activity. Drones and robots also present still-unresolved questions.[6] Profound issues of mission focus are also up for grabs – whether the CIA will continue to be dominated by its para-military side,[7] and whether the National Security Agency ("NSA") is destined to remain essentially a targeting service for a war machine at the expense of its national intelligence mission.[8] Distinguishing domestic from foreign communications is increasingly

5. JOEL BRENNER, AMERICA THE VULNERABLE, INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE at 127-53 (2011). The near-monopoly of nation-states over the means of intelligence gathering was actually an anomaly; we are returning to the historical norm. *Id*. at 190-199.

6. *E.g*., George R. Lucas, Jr., *Automated Warfare*, 25 STAN. L. & POL'Y REV. 317, 327 (2014).

7. *See, e.g*., Jane Harman, *Disrupting the Intelligence Community: America's Spy Agencies Need an Upgrade*, FOREIGN AFFAIRS, March–April 2015, https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community [http://web.archive.org/web/20150823124519/https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community].

8. *See* Dana Priest, *NSA Growth Fueled by Need to Target Terrorists*, WASH. POST (July 21, 2013), https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html; MICHAEL V. HAYDEN, PLAYING TO THE EDGE: AMERICAN INTELLIGENCE IN THE AGE OF TERROR 329 (2016) ("Years after I left government, I reviewed my Thursday morning briefing scripts for the President and was struck by how much they focused on terrorism and within terrorism how much they were about South Asia – Pakistan

difficult, heightening the need to regulate this aspect of foreign intelligence operations.[9]

Opening a book entitled *The Future of Foreign Intelligence*, this is the platter of issues one would expect on the table. But from this menu, the only dishes Professor Donohue serves up are the government's access to domestic digital data and the legal difficulties that arise from the inevitable mingling of domestic and foreign communications. Her book thus has little to do with the future of foreign intelligence, and rather than evaluate it as such, we will do better to accept it as the book her subtitle accurately describes: *Privacy and Surveillance in the Digital Age*. This is not a mere quibble about a title. Her argument is infected with a fundamental confusion between the scope and purpose of the Foreign Intelligence Surveillance Act ("FISA") and the general regulation of foreign intelligence, and that confusion is reflected in the title. In any case, privacy and surveillance are topic enough for a brief but passionate argument about the constraints (or as she would say, the lack of constraints) on the government's ability to vacuum up everyone's digital exhaust. Professor Donohue shapes this conversation through her teaching and as one of a handful of *amici curiae* appointed to advise the Foreign Intelligence Surveillance Court ("FISC") in cases of broad applicability. On these issues her views demand respectful attention.

I. THE ARGUMENT

Her arrows are aimed chiefly at two specific targets. The first is the Supreme Court's "third-party doctrine," which denies Americans a constitutionally based privacy interest in data they give to third parties, including common carriers and other digital platforms that provide essential services. I enlarge her attack on this doctrine.

---

and Afghanistan"); Harman, *supra* note 7 at 105 ("What role does that leave for the NSA? Its top priorities should be code-making, code-breaking, and cyberwarfare. Washington will still need the capacity to penetrate secure state networks and prevent its enemies, state and nonstate, from doing the same. Although the NSA has demonstrated abilities in this sphere, it needs to focus on keeping pace with talented Chinese, North Korean, Russian, and nonstate hackers."). Drawing causal connections between NSA's current priorities and missed opportunities is of course difficult. But in just the last few years, many have criticized America's spies for failing to predict national shifts abroad. *See, e.g.*, Stephen Blank, *Turkey: Another US Intelligence Failure*, ATLANTIC COUNCIL (July 20, 2016), http://www.atlanticcouncil.org/blogs/ukrainealert/turkey-another-us-intelligence-failure; James S. Robbins, *American Intelligence Failure In Syria*, USA TODAY (Oct. 14, 2015), http://www.usatoday.com/story/opinion/2015/10/14/syria-russia-islamic-state-intelligence-column/73861676/; John Crawley, *U.S. Intelligence Under Fire Over Ukraine*, CNN (Mar. 5, 2014), http://www.cnn.com/2014/03/05/politics/ukraine-u-s-intelligence/.

9. *See also* Michael Morell, *The Importance of Intelligence* , AUSTRALIAN STRATEGIC POLICY INSTITUTE: THE STRATEGIST (Aug. 31, 2016), http://www.aspistrategist.org.au/the-importance-of-intelligence/; HAYDEN, *supra* note 8, at 422 ("Long before Snowden, I was asking CIA's civilian advisory board 'Will America be able to conduct espionage in the future inside a broader political culture that every day demands more transparency and more public accountability from every aspect of national life?' The board studied it for a while and then reported back that they had their doubts.").

Her second major target is the 2008 amendments to the Foreign Intelligence Surveillance Act of 2008[10] (the "FISA Amendments Act" or "FAA"). That law allowed the NSA to collect, without a warrant, communications between targeted foreign citizens and Americans. She and I agree reforms are needed. But she would go further than I would by subjecting foreign intelligence collection to strict warrant requirements. That proposal misunderstands FISA's purpose and constitutional limitations.

Professor Donohue also presents a jaundiced but, as I will explain, undeveloped view of the area of government operations known as intelligence oversight. Finally, she contends that criminal law and the law governing intelligence gathering have little or nothing to do with one another and that the distinction between them is both meaningful and clear. Her most startling and potentially consequential proposal is to resurrect that doctrine by re-erecting "The Wall" that, until 2002, required the complete separation of criminal investigations from all information gathered using foreign intelligence sources and methods. In my view, the destruction of that barrier was one of the most significant and desirable changes to the organization of the federal government following the attacks of 9/11.

I examine her arguments in this order.

II. THIRD-PARTY DOCTRINE AND METADATA

In the early 1970s, federal authorities served subpoenas on two banks with which a bootlegger named Miller did business. The banks complied. Miller moved unsuccessfully to suppress the banks' evidence on the grounds that it had been seized without warrants in violation of the Fourth Amendment. He was later convicted of various federal crimes. The Court of Appeals for the Fifth Circuit overturned his conviction, but the Supreme Court reversed. The Court held that:

1. the subpoenaed papers were the bank's business records;
2. the bank was required to maintain them under the Bank Secrecy Act of 1970;[11] and
3. Miller had no reasonable expectation of privacy either in the bank's copy of the records or in the original checks, which were negotiable instruments used in commercial transactions.[12]

Miller's holding could easily have been confined to negotiable instruments or to business records maintained under statute. But three years later, in *Smith v. Maryland*[13] the Supreme Court expanded *Miller* to cover any information given to any third party. Petitioner Smith had been convicted of robbery based in part

10. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435, 2436.
11. 12 U.S.C. § 1829b(d) (2012).
12. United States v. Miller, 425 U.S. 435, 442 (1976).
13. Smith v. Maryland, 442 U.S. 735 (1979).

on telephone numbers collected from a pen register placed on his phone without a warrant. Holding that Smith had no Fourth Amendment interest in the phone company's business records, the Court expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial."[14] For good measure the Court added that if Smith did have such an expectation of privacy, it was not one society was prepared to recognize as reasonable. Smith had "voluntarily conveyed" his dialing information to the phone company[15] and had therefore "assumed the risk" that the company would reveal the information to the police. We now had a broad, clearly articulated third-party doctrine: "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[16]

Miller and *Smith* were both based on the "reasonable expectation of privacy" test of *Katz v. United States*.[17] With rare exceptions,[18] lower courts have repeatedly reaffirmed the third-party doctrine. But as Professor Donohue makes clear, that doctrine no longer protects reasonable expectations of privacy. During the 1970s, people only shared information with third parties (other than the bank and the phone company) by handing a box of papers to their lawyers, accountants, or business associates. There were no permanent records of people's messages to their family and friends. Today, by contrast, nearly all information is routinely digitized and shared with cloud service providers. If your smartphone or laptop is backed up by Google, Apple, or anyone else, you have no constitutional privacy interest in its contents. People increasingly keep all manner of personal and business records "on" their smartphones, which combine the features of filing cabinets, photo albums, contact directories, diaries, credit cards, and so forth all in one place. Dating apps record people's sexual preferences and romantic liaisons. And unlike the defendant's phone in *Smith*, which was tethered to a wall, mobile phones move freely.[19] Mobile phones, especially smartphones, are tracking devices. Uber and Lyft, the weather app, the city transportation app, and many others have little or no value if they do not know exactly where you are. Your mobile phone must also know where you are at all times in order to connect your calls, so it constantly communicates with cell towers even when you're not on the phone.

14. *Id*. at 744.

15. It would have been more accurate to say that his data had been automatically captured by a common carrier which at that time was still a monopolist of an essential means of communication.

16. *Smith*, 442 U.S. at 744-45.

17. 389 U.S. 347 (1967).

18. *See, e.g*., Klayman v. Obama, 957 F. Supp. 2d 1, 44 (D.D.C., 2013), *vacated*, 800 F.3d 559, 562 (D.C. Cir. 2015) (per curiam).

19. Americans are fast giving up landlines. *See* Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey*, CTRS. FOR DISEASE CONTROL (December 2014), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf ("Preliminary results from the January–June 2014 National Health Interview Survey (NHIS) indicate that the number of American homes with only wireless telephones continues to grow. More than two in every five American homes (44.0%) had only wireless telephones . . . . during the first half of 2014—an increase of 3.0 percentage points since the second half of 2013. More than one-half of all adults aged 18-44 and of children under 18 were living in wireless-only households.").

Companies keep this data and often sell it. Our phones thus record not merely where we are now, but where we have been and how long we were there. Soon, thanks to the third-party doctrine, no one will have a reasonable expectation of privacy in almost anything.[20]

Technological developments notwithstanding, the third-part doctrine was also bad law to begin with. It treats a substantive constitutional right as if it were merely an evidentiary privilege that is automatically lost when shared with anyone else. That view does not reflect reasonable expectations of privacy, and it never did. If you disclose to a third party an otherwise privileged conversation with your lawyer, you lose the privilege. But this is merely a rule of evidence. We do not use the subsequent third-party disclosure to declare that the client had no right to share information in confidence with the lawyer in the first place. Rather, we recognize that lawyer and client, like doctor and patient, communicate in a zone of confidence. The third-party doctrine recognizes no such zone for information that ordinary people must, as a necessity of life, share with companies that promise to protect their privacy.[21] In *Miller*, for example, the petitioner's bankers testified that they regarded their customers' records as confidential,[22] and the prosecution admitted as much.[23] But *Miller*'s holding effectively eliminated any such confidence that reasonable customers had.[24] In short, the reasonable expectation test of *Katz* would have fit the facts in *Miller* like a glove, if the Court had only tried it on.[25]

---

20. Cisco forecasts that cloud usage will grow three-fold from 2014-2019, and that by 2019, "more than four-fifths (86 percent) of workloads will be processed by cloud data centers; 14 percent will be processed by traditional data centers." CISCO, *Cisco Global Cloud Index: Forecast and Methodology, 2015–2020* (2016), [http://web.archive.org/web/20160204180157/http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf]. Individuals and businesses are moving to third-party cloud services, particularly in the United States. *See, e.g.*, STATISTA, *United States: Brand preferences for cloud data storage in Q1 2016, by income*, https://www.statista.com/statistics/550987/united-states-brand-preferences-for-cloud-data-storage-by-income/. This trend is bound to grow worldwide. In 2015, 3.37 billion people, or 46.4 percent of the world's population, had Internet access. In North America, the penetration percentage was 87.9 percent. Even in the least connected places, access is growing at a dramatic rate. INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm. Facebook alone claimed 2 billion monthly active users as of June 2017. *See* Josh Constine, *Facebook now has 2 Billion Monthly Users. . . And Responsibility*, TECHCRUNCH.COM (June 27, 2017), https://techcrunch.com/2017/06/27/facebook-2-billion-users/.

21. As the doctor-patient example illustrates, we know how to create such a zone even when it has no constitutional underpinning. *See also* Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (building on breach of trust cases in developing a proposed right to privacy at common law, breach of trust may be ready for a come-back in the privacy wars).

22. 425 U.S. at 449.

23. *Id*. at 448-49 (Brennan, J., dissenting).

24. See *Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

25. Nor is it sufficient to say that the bank was obliged to keep the records by the Bank Secrecy Act, because a requirement to preserve records to make them amenable to legal process does not prescribe the process by which the government may obtain them. Financial Recordkeeping and Reporting of

Miller and *Smith* thus represent an attempt to define a substantive right through a mechanical, inapt test borrowed consciously or unconsciously from the law of evidence. The attempt was always flawed in principle. But thanks to technological developments putting virtually all our private information in third parties' hands, it now produces intolerable results. So Professor Donohue is right: Supreme Court precedent does not protect ordinary citizens from government's unreasonable intrusions into private lives. It requires re-thinking.

Several members of the Court appear to agree, as Justice Scalia's opinion for the Court and the concurrences in *Jones v. United States*[26] suggest. *Jones* presented the question whether attaching a GPS tracking device to a man's automobile, and subsequently using that device to monitor the vehicle's movements on public streets, constituted a Fourth Amendment search or seizure. A five-justice majority declined to apply the rule on the narrow ground that, notwithstanding *Katz*'s expectation of privacy test, the government had trespassed in affixing the device to the vehicle.[27] The majority knew that its disposition of the case left the hard question lurking in the wings: "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[28] Justice Sotomayor concurred but issued a separate opinion to emphasize the larger issue. "I would ask," she wrote, "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." Her implication was clear: "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[29] Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, had the same concern. "[I]f long- term monitoring can be accomplished without committing a technical trespass — suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car — the Court's theory would provide no protection."[30] We thus had all nine members of the Court expressing discomfort both with the third-party doctrine and its interplay with *Katz*.[31]

Currency and Foreign Transactions Act of 1970, 31 U.S.C. § 5311 (2012). If these records are entitled to Fourth Amendment protection, the legislature had no more right to violate that right than did the executive. U.S. Const. amend. IV. The assumption-of-risk rationale is even flimsier, as one could as well say that a party assumes the risk that anyone owing a duty of confidence, including a lawyer or physician or spouse, would breach it.

26. 565 U.S. 400 (2012).

27. "[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Id*. at 409.

28. *Id*. at 412.

29. *Id*. at 416–17 (Sotomayor, J., concurring).

30. *Id*. at 425 (Alito, J., concurring in the judgment). Justice Alito also suggested that the Congress rather than the courts should take the lead in this area. *Id*. at 427-28.

31. Two years later, a unanimous Court held that digital technology required changes to traditional Fourth Amendment doctrine in *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("Finally, there is an

Jones may mark the beginning of the end for an across-the-board third-party doctrine, but the end is unlikely to come at a single stroke. Congress has displayed no enthusiasm for legislating in this area, and courts will be slow to abandon a mechanically applied doctrine that produces clear results.[32] But doctrinal clarity costs too much in today's digital economy. The third-party doctrine destroys information privacy and yields unreasonable results. It is premised on technologically obsolete assumptions about the world – a point that Professor Donohue makes wonderfully clear – and it was unsound from the beginning.

In its time, *Katz* expanded individual rights by holding that citizens enjoy a zone of privacy that moves with them. But its reasonable expectation standard should be re-thought. On the one hand, it is insufficient to deal with technological advances that are rapidly destroying expectations of privacy that still seem reasonable to many people; on the other hand, it could be useful in fashioning protections for information that must, as a practical matter, be shared with third parties. Professor Donohue thinks we may be in "a pre-*Katz* moment," ripe for a doctrinal shift. When a majority of the Court declares that "Fourth Amendment rights do not rise or fall with the *Katz* formulation,"[33†] she's probably right.

III. COLLECTION UNDER FISA

Professor Donohue mounts three principal attacks on the FAA. *First*, it authorizes the collection of bulk electronic metadata without a warrant, by which she apparently means a Title III warrant.[34] She asserts this practice is unconstitutional, by which she presumably means that in her view it should be unconstitutional, because she knows that the third-party doctrine, just discussed, denies citizens a Fourth Amendment right to privacy in communications metadata.[35]

---

element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. . . . Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate.").

32. Abandoning the third-party doctrine per se could also have implications for the law governing the use of informants by the government. *See* United States v. White, 401 U.S. 745 (1971).

33. *Jones*, 565 U.S. at 406.

† Since the writing of this review, a divided Supreme Court further eroded the third-party doctrine, holding that the seizure of the defendant's cell-site records over a 127-day period required a Title III warrant. Carpenter v. United States, 138 S. Ct. 2206 (2018).

34. Professor Donohue uses the term "warrant" to refer to both Title III and FISA orders. Under FISA, surveillance orders are formally known simply as orders rather than warrants, apparently because the drafters of that statute wished to make clear that the President's Article II power to collect foreign intelligence was not subject to the Fourth Amendment. I follow the statutory usage. The distinction can be significant. *See In re* Warrant to Search a Certain E-Mail Account, 829 F.3d 197, 214 (2d Cir. July 14, 2016), *vacated sub nom.*, United States v. Microsoft Corp., 138 S.Ct. 1186 (2018).

35. *See, e.g.*, United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016), *cert granted*, 137 S. Ct. 2211 (2017); *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 136 (3d Cir. 2015); United States v. Guerrero, 768 F.3d 351, 358-59 (5th Cir. 2014).

Second, she argues that a FISA order that authorizes the collection of large numbers of international communications that begin or terminate in the United States between foreign persons overseas who are associated with terrorism is unconstitutional. Instead, she believes a FISA order must be restricted to a single, particularized call or message. She provides no constitutional foundation for her position, and there is none.

Third, she argues that the government's unrestrained ability to retain and examine lawfully collected intercepts of conversations involving U.S. Persons under section 702 is unconstitutional and should be regulated. Here again Professor Donohue's arguments about constitutionality are perplexing, at least to this reader, because they are not based on a parsing of constitutional text and Supreme Court decisions as they apply to particular parts of FISA. Instead, she offers a lively disquisition, fully a quarter of the book, on the origins of the Fourth Amendment and the history of general warrants in the run-up to the American Revolution.[36] As a former member of the guild of legal historians, I found this background relevant but, standing alone, unpersuasive. Nevertheless, I agree with her that access to stored 702 data should be regulated, though I doubt we agree on how to do it.

While I find common ground with several of Professor Donohue's specific proposals for further FISA reform, I see two major weaknesses in the foundation of her attacks on FISA collection and thus with her broader argument. The first weakness – in my view, error – is constitutional and legal. It concerns the scope and purpose of the FISA statute, which were limited in their reach by the President's independent constitutional authority to collect foreign intelligence. The second weakness is partly technological and partly a result of failing to acknowledge the altered intelligence challenge in the form of metastasized terrorism that confronts anyone, regardless of political inclination, who wishes to regulate the monitoring of communications. Before addressing these points, however, a brief history of bulk metadata and FISA collection since the attacks is in order.

A. Origins of Bulk Collection and the "702 Program"

Shortly after 9/11, the Bush Administration put in place a surveillance program called STELLAR WIND. That program authorized NSA to intercept communications between persons overseas with known terrorist affiliations and persons in the United States. It also authorized the collection of bulk metadata (that is, information about a communication but not its contents)[37] from U.S. telecommunications

36. Characterizing arguably overbroad orders as general warrants strikes me as wildly exaggerated, and it would no doubt surprise the judges of the FISC, who spend considerable effort crafting restraints they appear to find meaningful. She concedes, "There are some differences between the general warrants about which the Framers were concerned and those that mark the realm of foreign intelligence today." DONOHUE, *supra* note 2, at 94. Among other things, FISA orders are limited in scope and must have a foreign intelligence nexus.

37. Offices of the Inspectors General of the Department of Defense, Departmet of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, *Report on the President's Surveillance Program* (the *"Joint IG Report"*) (July 2009) v. 1 at 8, available

carriers in order to understand who the persons on the U.S. end of those calls were communicating with. Through link analysis, these metadata connections could be followed for three "hops," thereby gathering call information about a huge number of domestic calls. The program was authorized by Presidential order, outside the FISA structure. FISA at that time did not address metadata collection. Metadata analysis was beginning to play a critical role in wiping out terrorist networks overseas,[38] however, and the Bush Administration believed it would similarly be critical in rolling up any of those networks that extended into the United States.

By late 2003, however, some government officials had become concerned about the legal authority to collect bulk metadata.[39] Consequently, in July 2004 the collection of bulk *Internet* metadata quietly was moved under section 214 of the PATRIOT Act (which amended section 402 of FISA). That statute permits pen registers and trap-and-trace devices, but authorizations for such devices had previously been used only for specific telephone numbers or Internet addresses. However, then-chief judge of the FISC District Judge Colleen Kollar-Kotelly was persuaded that the statute could be used to collect Internet metadata in bulk in real time.[40] Suffice it to say that this was a novel and controversial interpretation of section 214 that vastly expanded the scope of the government's statutory power to collect bulk metadata. And it occurred in secret.

The portion of STELLAR WIND relating to the interception of the content of U.S.-foreign calls (but not the portion relating to bulk metadata collection) was exposed by the *New York Times* in December 2005. The disclosure increased the sense of urgency within the Justice Department's Office of Legal Counsel that the telephony portion of metadata collection should also be given a firmer and explicit statutory basis.[41] In May 2006 the collection of bulk *telephony* metadata

---

at https://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html, accessed May 21, 2018. Telecommunications metadata includes such information as the IP address of the other party to the communication, the path taken by the communication, and its duration. Id.

38. HAYDEN, *supra* note 8, at 76. For a description of how this played out in Iraq, *see*, Shane Harris, *How the NSA Became a Killing Machine*, THE DAILY BEAST (Nov. 9, 2014), http://www.thedailybeast.com/articles/2014/11/09/how-the-nsa-sorta-won-the-last-iraq-war.html. For a discussion of the benefits of NSA programs, *see generally* John McLaughlin, *NSA Intelligence-Gathering Programs Keep Us Safe*, THE WASH. POST (Jan. 2, 2014), https://www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html?utm_term=.3ef8662883bd; Philip Mudd, *Mapping Terror Networks: Why Metadata Matters*, THE WALL STREET JOURNAL (Dec. 29, 2013), http://www.wsj.com/articles/SB10001424052702304367204579270472690053740.

39. *See* BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY 151 (2008); JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 181–82 (2007).

40. *See* Undated Opinion by Judge Colleen Kollar-Kotelly Declassified Without Date or Caption, at 20-21 (FISA Ct.), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

41. Professor Donohue would deny that the program had *any* statutory basis. She dismisses without discussion the Bush administration's reliance on the Authorization for Use of Military Force ("AUMF") – as if it were frivolous to argue that intelligence collection against persons in communication with the enemy is a normal incident of war-making authority. *See* Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001). For the administration's arguments about its effect, *see* U.S. Dep't of Justice, Att'y Gen., Opinion Letter on Legal Authorities Supporting the Activities of the National Security Agency Described by the President (January 19, 2006), https://www.justice.gov/sites/default/files/olc/opinions/attachments/2015/05/29/op-olc-v030-p0001.pdf. For another view of the limits of the

was moved under section 215 of the PATRIOT Act, which had amended section 501 of FISA. That statute authorized the government to obtain certain business records through legal process.[42] Technically, this meant that NSA stopped "collecting" telephony metadata in real time as part of its intelligence mission and was instead merely obtaining business records through legal process. Practically speaking, however, there was no difference because the business records went to the government more or less as they were generated. Thanks to the third-party doctrine discussed above, this program was entirely constitutional.

The following year, in August 2007, Congress passed the Protect America Act ("PAA") to provide clear statutory authority to collect the *content* of communications between a person overseas and a person in the United States,[43] but that authority expired after only eighteen months. After a hiatus, Congress passed the FAA in July 2008. It remains in effect. Unlike the original FISA, the FAA required a FISA order before a U.S. Person could be targeted, even if that person was overseas, in circumstances where a Title III warrant would be required in a criminal case.[44] This was a significant expansion of FISA's regulatory scope and, to that extent, an expansion of civil liberty.

But the FAA also created what is often called the "702 Program," which is one of Professor Donohue's chief targets. As amended by the FAA,[45] Section 702 permits "the targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[46] In this context, "foreign intelligence information" means the contents of communications and not merely metadata. A FISA order is not required for this collection. Rather, the Attorney General and the Director of National Intelligence select the information to "target" and then direct electronic communications providers to turn over this information. If the government has "reasonable articulable suspicion" that a foreign person has a terrorist connection, that person may be targeted when the foreign person communicates with someone in the United States. If, for example, a known terrorist overseas is having conversations with a U.S. Person in Minneapolis, our agencies may collect that communication. However, an agency may not do so if the purpose of the collection is really to target the person in Minneapolis. That would be "reverse targeting." Electronic communications

President's Article II power, *see* David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb – A Constitutional History*, 121 HARV. L. REV. 941 (2008).

42. Internet service providers, unlike phone companies, do not keep business records of communication data. Hence this change was limited to the telephony portion of the metadata program.

43. Protect America Act of 2007, Pub. L. No. 110-55, § 105B, 121 Stat. 552. The PAA also dropped the requirement of a FISA order for foreign-to-foreign communications that happened to "transit" the United States. § 105A. Under the old rule, NSA could freely collect that same communication if it captured it, say, from a satellite signal or a cable overseas, but it needed a FISA order if it captured the communication off a wire in the United States. *Compare* 50 U.S.C. § 1801(f)(2) (2006), *with* § 1801(f)(3) (2006). That requirement protected no one's privacy. It merely regulated the place of interception.

44. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703(a)(1), 122 Stat. 2436, 2448.

45. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438-48 (codified as amended at 50 U.S.C. § 1881 (2015)).

46. § 702(a).

service providers may challenge these directives before the FISC and appeal to the FISA Court of Review. By long-standing practice, the database of 702 information may be accessed at any time by intelligence or law enforcement officials without court approval and may be queried with any search term, including U.S. Person identifiers.

Professor Donohue objects vehemently to this program. It appears she would subject 702 collection to the criminal warrant process of Title III. In my view, she reaches this position based on a misunderstanding of FISA's purpose and an unsupportable view of the constitutional requirements governing foreign intelligence collection.

B. FISA's Purpose and Constitutional Requirements

Professor Donohue confuses FISA's purpose with the general regulation of foreign intelligence. This may account for the book's inapt title. She asserts: "FISA represented the culmination of a multibranch, multiyear, cross-party initiative *directed at bringing the collection of foreign intelligence within a circumscribed legal framework*" (emphasis added).[47] This is not true. Foreign intelligence collection is a broad category, occurring in many ways through a variety of human and technological means and gathered against targets that are overwhelmingly outside the United States. FISA brought under law one element of that enterprise, namely, the collection of (i) *electronic* foreign intelligence (ii) taken off a wire or from a radio signal (iii) in the United States. That slice of foreign intelligence, because it was collected domestically, could be (and sometimes had been) used to avoid the search-and-seizure strictures of the Fourth Amendment. In the wake of the Church Committee hearings in 1976, Congress enacted FISA to prohibit such evasions.

The constitutional difficulty with Professor Donohue's argument about collection under FISA is inseparable from this issue of FISA's purpose. Contrary to her assertions, foreign intelligence taken from domestic telecommunication networks involves powers granted to *two* branches of government.[48] Under Article I, Congress has the power to regulate interstate and foreign commerce, including telecommunications (at least when used in commerce).[49] But Congress has long deferred to the view that foreign intelligence collection is an executive function

47. DONOHUE, *supra* note 2, at 10.

48. Professor Donohue asserts without citation, "Congress and the courts … had previously considered and declined to recognize claims to Article II authority to conduct foreign intelligence gathering inside the United States absent a warrant." *Id*. at 23. If this is a reference to *United States v. United States District Court*, 407 U.S. 297 (1972) ("*Keith*"), it is wrong. *See Keith*, 407 U.S. at 322–23 ("[T]his case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues involved with respect to activities of foreign powers or their agents.").

49. U.S. Const. art. I, § 8, cl. 3; LETTER FROM CONSTITUTIONAL LAW SCHOLARS AND FORMER GOVERNMENT OFFICIALS TO MEMBERS OF CONGRESS 7 (July 14, 2006), https://balkin.blogspot.com/NSA.Hamdan.July14.FINAL.pdf.

vested in the President under Article II of the Constitution,[50] even though there is no express provision for it in Article II.[51] Indeed, the President's power to monitor communications entering and leaving the country has been recognized since Washington's administration.[52] This is why Congress, in enacting FISA, recognized a reasonableness limitation on its power to control communications entering or leaving the country if they concerned foreign intelligence.[53] It certainly did not contest the principle that the President has the "*exclusive function* to command the instruments of national force, at least when turned against the outside world for the security of our society."[54] The Bush Administration, by acting as if it had the power to conduct the STELLAR WIND program on a long-term, non-

50. See DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF NSA DESCRIBED BY THE PRESIDENT (2006), https://epic.org/privacy/terrorism/fisa/doj11906wp.pdf. The Senate Intelligence Committee also acknowledged that the law was not intended to cover "electronic surveillance abroad." S. Rep. No. 95-701, at 7 (1978). While "protect[ing] the rights of Americans abroad from improper electronic surveillance" might raise constitutional issues, it never even occurred to the Committee that the same could be said of the surveillance of non–U.S. Persons. *Id*. at 7 n.2.

51. *See* Jack Goldsmith, Zivotofsky II *as Precedent in the Executive Branch*, 129 HARV. L. REV. 112, 114 (2015) ("Until *Zivotofsky II*, [executive branch] lawyers had to rely on shards of judicial dicta, in addition to executive branch precedents and practices, in assessing the validity of foreign relations statutes thought to intrude on executive power."); *see also* JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 72 (2007) ("The president's intelligence authority is derived from his enumerated authorities as commander in chief and chief executive, as well as his collective authority over foreign affairs, and to take care that the laws be faithfully executed. As intelligence is an integral function of military command and the conduct of foreign affairs, as a general matter the president has broad derived authority over the intelligence function. Congress has recognized as much in statute.").

52. *See* CHRISTOPHER ANDREW, FOR THE PRESIDENT'S EYES ONLY: SECRET INTELLIGENCE AND THE AMERICAN PRESIDENCY FROM WASHINGTON TO BUSH 6-12 (1995); *see also* LOUIS HENKIN, FOREIGN AFFAIRS AND THE UNITED STATES CONSTITUTION 111 (2d ed. 1996) ("From our national beginnings, Congress has recognized the President's exclusive responsibility for gathering intelligence, as an extension of his role as 'sole organ' and his traditional function as 'the eyes and ears' of the United States."); BAKER, *supra* note 51, at 71 ("Presidents have engaged in the practice of domestic and foreign intelligence collection since the advent of the United States. . . . [I]n the landline age, presidents routinely authorized electronic surveillance (wiretapping) to collect foreign intelligence.").

53. *See* S. REP. NO. 95-604, at 16 (1977) ("The basis for this legislation is the understanding – concurred in by the Attorney General – that even if the President has an 'inherent' constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a *reasonable* warrant procedure governing foreign intelligence surveillance.") (emphasis added); *see id*. at 7 ("The Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States . . .").

54. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 645 (1952) (Jackson, J., concurring) (emphasis added); *cf*. Zivotofsky *ex rel* . Zivotofsky v. Kerry, 135 S. Ct. 2076, 2094 ("Throughout the legislative process, however, no one raised a serious question regarding the President's exclusive authority to recognize the PRC – or to decline to grant formal recognition to Taiwan. Rather, Congress accepted the President's recognition determination as a completed, lawful act; and it proceeded to outline the trade and policy provisions that, in its judgment, were appropriate in light of that decision. This history confirms the Court's conclusion in the instant case that the power to recognize or decline to recognize a foreign state and its territorial bounds resides in the President alone.") (internal citations omitted).

emergency basis outside the FISA framework,[55] failed to recognize that it shared constitutional authority over activities involving the telecommunications of the American people. In a mirror image of that error, former Senator Russ Feingold was also wrong to assert, in a flight of rhetorical excess with which Professor Donohue is much enamored, that electronic foreign intelligence is an area of "absolutely clear, exclusive authority adopted by Congress ...."[56] This is wrong. Like Senator Feingold, Professor Donohue ignores FISA's purpose and history, which probably accounts for her failure to explain why the standard for obtaining a FISA order, which she criticizes repeatedly, differs from the Title III warrant standard.[57]

Title III was passed in 1968 in response to the Supreme Court's *Katz* decision one year earlier.[58] Congress reacted by crafting standards for issuing surveillance warrants sufficient to meet Fourth Amendment standards in criminal cases. Under Title III, a magistrate may issue a warrant authorizing the executive to acquire the contents of a wire, oral, or electronic communication if:

(1) "there is probable cause for belief that an individual is committing, has committed, or is about to commit" certain crimes; and

(2) "there is probable cause for belief that particular communications concerning that offense will be obtained through such interception"; and

(3) "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous"; and

(4) (in most cases) "there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."[59]

---

55. The first STELLAR WIND order was signed on October 4, 2001. Thirty-three months later, on July 14, 2004, a FISA order was entered under which the program began to be transitioned to FISA. *Joint IG Report*, v. 1 at 7, 52.

56. DONOHUE, *supra* note 2, at 36 (citing 154 CONG. REC. S6382 (daily ed. July 8, 2008) (statement of Sen. Feingold)); *cf. Youngstown*, 343 U.S. at 635-38 (1952) (Jackson, J., concurring). *Youngstown* involved competing Congressional and Executive authority where President Truman had ordered the seizure of steel mills on national security grounds during the Korean War. Justice Jackson proposed three categories of presidential acts corresponding to three levels of authority: Category One involved acts taken "pursuant to an express or implied authorization of Congress," Category Two involved acts taken in the "absence of a congressional grant or denial of authority," and Category Three involved acts taken in defiance of the express or implied will of Congress. *Id.*

57. 18 U.S.C. § 2518 (2012).

58. Katz v. United States, 389 U.S. 347 (1967), holding that a government interception of a telephone call required a warrant. At the time of the decision, there were no statutory standards for issuing warrants in such cases; hence the need for Title III.

59. 18 U.S.C. § 2518(3) (2012).

Would the imposition of these requirements on foreign intelligence collection be unreasonable? Surely it would be, because it would irrationally assume that foreign intelligence may not be collected in the United States unless there were probable cause to believe a crime were involved, and because it would be an unreasonable constraint on Executive power. A great deal of foreign intelligence does not involve the commission of crimes cognizable in U.S. courts. The Supreme Court has recognized that there is no constitutional obligation to apply these statutory requirements to "domestic security surveillance [, which] may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[60] The Court also doubted that such requirements applied to collection "with respect to activities of foreign powers or their agents."[61] If they did apply, we would arguably be in Justice Jackson's third category, in which the President's power is at its lowest ebb. "Courts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject."[62] Justice Jackson was an eminently practical man. As he said, "any actual test of power is likely to depend on the imperatives of events and contemporary imponderables, rather than on abstract theories of law."[63] He might therefore simply say that where two lawful but different powers both impinge on a single area of governmental activity, Congress must exercise its power – and Congress' power must be construed – in a manner that does not unreasonably impinge on the President's authority and, in this case, on his duty to protect the nation. There are limits on what Congress can do.

In contrast to Title III, the FISA standard to which Professor Donohue objects was created to deal with an entirely different problem than the investigation of crime, namely, the potential misuse of the President's power to collect foreign intelligence in the United States. The President has the power to collect foreign intelligence *even in the United States* without a search warrant.[64] A surveillance operation against a foreign embassy in Washington, for example, has never required a Title III warrant; nor does it now require a FISA order.[65] However, if that power is abused to collect against citizens on the pretext, for example, that the citizen was or might be a member of a foreign-controlled entity, the Fourth Amendment's warrant requirement would be effectively evaded. The purpose of the FISA standard was to police such evasion, not to impose a criminal-law

60. 407 U.S. at 322.

61. *Id.*

62. *Youngstown*, 343 U.S. at 637-38.

63. *Id.* at 637.

64. *See Katz*, 389 U.S. at 363 (1967) (White, J., concurring) ("Wiretapping to protect the security of the Nation has been authorized by successive Presidents"); *United States v. United States Dist. Ct. for E.D. of Mich.*, 444 F.2d 651, 669–71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) ("[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.").

65. 50 U.S.C. § 1822(a) (2012).

standard on foreign intelligence collection.[66] This is why, under FISA, an interception order may issue if the court finds there is probable cause to believe only that "(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power . . .; (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power"; and certain procedures are followed to minimize inadvertent collection.[67] Professor Donohue gets this history and purpose all wrong. She writes, "The point of having lowered [FISA] standards [compared to Title III] was to facilitate the collection of information about significant threats to national security."[68] No, it wasn't. Congress was not facilitating executive power; it was regulating a portion of that power severely and for the first time.

Professor Donohue is on stronger ground in her criticism of the lowered standard for the production of business records under FISA. The statute was amended in 2015 so that the government was required merely to certify, not to demonstrate, to the FISC that the records sought were merely relevant to an authorized investigation "to protect against international terrorism or clandestine intelligence activities."[69] In such a case, the magistrate may not inquire further and *must* enter the order. Professor Donohue asserts that the statute as it now stands is unconstitutional on its face, but that would be true only if persons had a constitutionally recognized privacy interest in data given to third parties. At present they do not. I would agree, however, that the relaxed standard has produced a British-style regime of seizure orders independent of the judiciary, and I would strengthen the standard to require the FISC judge to determine that the government has a factual basis for its assertion.[70]

The statute also creates too much room for evasion of the Title III warrant standard and may thus be unconstitutional *as applied*, even under *Smith*. Suppose the FBI wanted to compel the production of the business records of an American citizen who was not an agent of a foreign power but may have been colluding with a foreign agent in a *different* criminal scheme. The government could get a production order without having to obtain a Title III warrant. It would simply

66. *Compare* S. REP. NO. 95-604, at 7 (1977) ("This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."), *with id.* at 18 ("[T]he Supreme Court noted that the reasons for domestic surveillance may differ from those justifying surveillance for domestic crimes and that, accordingly, 'different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate needs of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.'") (quoting *Keith*, 407 U.S. at 322).

67. 50 U.S.C. § 1805(a)(2) (2012).

68. DONOHUE, *supra* note 2, at 28.

69. 50 U.S.C. § 1861 (2012).

70. Professor Donohue also notes that the number of FISA orders now exceeds the number of Title III warrants per year. She asserts there is now a direct relationship between the decline in Title III warrants and the increase in FISA orders. DONOHUE, *supra* note 2, at 30. Her data suggest she may be correct, but a deeper inquiry (and better data) would be required to prove the point. One would think that the changed nature of the threat to the nation had something to do with it.

have to assert that evidence in the second scheme would somehow be useful in investigating the first one. That would be a dangerous infringement of constitutional protection against arbitrary executive power, and I hope it could not be defended merely by reference to the President's Article II powers.

C. Technology Effects

The advent of fiber-optic technology long before the passage of the FAA had the unintended effect of expanding the FISA's reach in irrational ways that are not widely understood. When FISA was enacted in 1978, telecommunications meant telephone and telegraph; there was no commercial Internet. Most long distance telecommunications employed a satellite link at some point in the transmission. That is, the electronic impulses representing a caller's voice on a call between, say, New York and Hamburg, or between Hamburg and Tokyo, were sent via radio frequency up to a satellite and then down from a satellite before finishing their journey by copper wire. If NSA wanted to target that communication, it could and usually did collect it though the air, probably from an overseas location, so it was not regulated by FISA. Even if it was collected from a location inside the country, FISA did not regulate the collection as long as no U.S. Person was the target.[71] With the advent of commercial fiber-optic cable on international lines beginning in 1988,[72] international call quality and reliability improved dramatically. But it also meant that the call between Hamburg and Tokyo was probably transmitted through a wire in the United States and thus became subject to FISA if collected in the United States, which was the easier and less risky way to do it. And given the U.S.-centric quality of the worldwide fiber-optic cable networks,[73] many other foreign-to-foreign communications also became subject to FISA. An unintended and perverse result was that a large volume of communications having nothing to do with FISA's purpose was brought under the act. This was a major nuisance, and it meant that in a significant class of cases, FISA was not protecting the privacy of U.S. Persons. It was merely regulating the place of collection. The PAA and then the FAA fixed that anomaly.

A typical fiber-optic trunk cable carries a petabit of data per second.[74] The government does not "tap" these cables using alligator clips in the basement wire closet of an apartment building like in a 1940s movie. Interception occurs at a

71. As originally passed in 1978, FISA defined "electronic surveillance" as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(f), 92 Stat. 1783, 1785.

72. Jeremiah Hayes, *A History of Transatlantic Cables*, IEEE COMM. MAG., Sept. 2008, at 42, 47.

73. *See Submarine Cable Map*, TELEGEOGRAPHY, http://www.submarinecablemap.com [http://web.archive.org/web/20160618040914/https://www.submarinecablemap.com] (last accessed June 18, 2016).

74. Matthew Peach, *NEC and Corning Achieve Petabit Optical Transmission*, OPTICS.ORG (Jan 22. 2013), http://optics.org/news/4/1/29.

carrier's switching station. If done by the police or FBI under a Title III warrant, the targeting must be precise because the government is forbidden from collecting anything outside the terms of the warrant. In the case of foreign intelligence, however, the situation is largely reversed. The President has the power to collect any communication likely to have foreign intelligence value, except that he must take care not to collect U.S. Persons' communications except as authorized by FISA. This reversal is based on constitutional requirements, but it offends Professor Donohue. She asserts that FISA orders should be limited to "*seizing or monitoring the content carried by a single telephone line, or to and from a particular computer address*."[75] The Constitution does not require the President to take such a dainty approach to foreign intelligence collection, and Congress appears to believe, correctly in my view, that it has no power to impose such a requirement.

IV. ACCESS TO STORED U.S. PERSON DATA

So much for electronic collection under section 702. Let us now turn to the analysis of 702 data and the access to data that intelligence analysis and law enforcement both require. As Professor Donohue correctly notes, the database of information collected under this section has become enormous. It contains the records of a publicly unknown but undoubtedly very large number of communications involving U.S. Persons in the United States communicating with intelligence targets overseas. Our intelligence agencies and the FBI may search that database using U.S. Person selectors for any purpose, without restraint, whenever they feel like it, even years after the collection occurred, even if they have lost interest in the overseas target. This state of affairs is merely the application of the long-standing rule that once a communication of a U.S. Person or anyone else has been lawfully collected, an agency may access that communication for any reason.

I share Professor Donohue's objection to this legal state of affairs under section 702, and the objection will be more powerful if placed in a broader context. We have entered an era when the terms on which the government may search lawfully gathered information are becoming as important as the terms on which the information may be lawfully collected. The government's access to vast quantities of information about U.S. Persons is growing dramatically. U.S. intelligence agencies already hold massive databases of information about Americans. They also have access to readily available commercial databases through a few keystrokes or through the purchase of proprietary databases. The data ocean is expanding as if propelled by a Digital Big Bang, and dealing with it requires automated analytic capabilities at a previously unimaginable scale. Most of this data ocean is held by private companies, whose ability to gather it and whose skill in analyzing it exceed the government's. The vast expansion of the private data market means that the government itself will gather *relatively* less data and purchase *relatively* more of it in open markets. Indeed, in some cases the ability to purchase commercial data in the open market will make restrictions on collection irrelevant.

75. DONOHUE, *supra* note 2, at 32 (emphasis added).

Historically our laws and regulations have controlled who may *collect* intelligence, whose communications may be collected, how they may be collected, and what may be collected.[76] Once information about U.S. Persons has been lawfully collected, we also regulate how and to whom it may disseminated, but we have not regulated the conditions or frequency under which the collecting agency may access or analyze it. Section 702 is merely an example of this historical way of doing business. The protections afforded to U.S. Persons through collection rules always seemed sufficient to protect our liberty. I predict this is going to change. We are probably at the threshold of a new era. In the future, we are likely to be at least as concerned with the state's ability to access information already collected, or available in the marketplace, as we have been with the conditions under which the state may collect it using its own resources.

Greater attention to data access as opposed to data collection will also be impelled by a change in intelligence agencies' mission. Their task is no longer simply to acquire the communications of known foreign agents or to hunt moles in their own organizations, as was the case throughout the Cold War. Knowing who the foreign targets were was relatively easy. Stealing their communications was hard.[77] That mission is now accompanied by a new one that has deep legal and public support, namely, to discover terrorist networks before they can wreak havoc. In the foreseeable future, this challenge will probably condition the intersection between government's intelligence gathering and citizens' rights more than any other factor, yet it strangely finds no place in this book. In pursuit of terrorists, stealing the secrets is usually the less difficult task. The harder and more important part is knowing who they are, and that involves access, under controlled conditions, to communications data in bulk – to both metadata and to lawfully collected intercepts – and sifting them for information with intelligence value. To a significant degree, therefore, the challenge in intelligence collection has been turned on its head. Whether we like it or not, from now on more and more information will be in government hands or easily available to government. Increasingly the questions will be: When can government look at it? And how can we police abuses?

V. OVERSIGHT

The subject of potential abuse – by which I mean intentionally or systematically unlawful intelligence collection[78] – brings us to the question of oversight,

76. *See, e.g.*, Exec. Order No. 12,333, United States Intelligence Activities, 3 C.F.R. 200 (1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008); 50 U.S.C. § 1801.

77. *See also* HAYDEN, *supra* note, 8 at 32 ("Intelligence [during the Cold War] was hard work, but it was difficult for our adversary to hide tank armies of Group Soviet Forces Germany or the vast Soviet ICBM fields in Siberia. That enemy was pretty easy to find. Just hard to kill. This was different. This enemy was relatively easy to kill. He was just very, very hard to find.").

78. Inadvertent collection (e.g., of U.S. Persons' communications in the course of lawful foreign intelligence collection) is anticipated by statute and is not abusive unless it is not mitigated as provided by statute. *See* 50 U.S.C. §1881(h) (2012).

but this is a subject on which Professor Donohue, after raising it, has little to say. She treats us to a tantalizing observation by Stanford's Professor Scott Sagan, whose work on nuclear weapons policy led him to conclude, in her words, that "the *more* protection one builds into a system, somewhat counterintuitively, the *less* secure it may become." This is a brilliant insight of remarkably limited value here, since hardly anyone (including Professor Sagan[79]) would argue the converse: That the less protection one builds into the system of intelligence oversight, the more secure it is likely to become. Indeed Professor Donohue wants "more robust oversight."[80] But she is vague on what that means. Her only concrete suggestion is to say it would be a good idea to have more people like her – amici curiae appointed by FISC – but this is what the USA Freedom Act actually did in 2015.

What Professor Sagan describes is a version of the shared responsibility trap, in which an actor with partial or redundant responsibility becomes lazy and inattentive in the belief that others have their eyes on the ball ("social shirking," he calls it).[81] As the former inspector general of the National Security Agency during the STELLAR WIND period, that's not how I saw intelligence oversight. My office had its hands full and was deeply involved not only in uncovering abuse after the fact (not usually involving intelligence collection, I might add) but also in preventing it. Different oversight mechanisms in different organizations are designed to accomplish different objectives – they are not redundant – and their critics usually pay insufficient attention to what the different parts are meant to do. It is unreasonable, say, to expect the House and Senate select committees on intelligence to monitor collection activities. Their responsibilities are strategic and general, not tactical and granular. In contrast, it would be reasonable for these budget authorizing committees to require that new collection capabilities be auditable to a standard agreeable to agency inspectors general, who are (or should be) able to monitor collection. But no oversight system will be perfect, and expecting perfection (usually with a handwringing reference to the unanswerable question, Who will watch the watchers?) leads only to the continual imposition of additional oversight mechanisms on top of one another, a tendency that expands the pool of unproductive employment opportunities at the expense of efficiency.

Expecting perfection also leads to what I call the Oversight Paradox: The closer one is to the activity being overseen, the more one will know about how it works, but the less one will be trusted; and the farther one is from the activity, the

79. Scott Sagan, *The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security*, 24 RISK ANALYSIS 935, 935-46 (2004) ("The implication of the argument, however, is not that redundancy never works in efforts to improve reliability and security. Moreover, the central policy lesson is not that the U.S. government should reject all proposals to place more security forces at nuclear facilities, given the heightened terrorist threat after the September 11, 2001 attacks. Instead, the lesson is that we need to be smarter in the way we think about redundancy.") (emphasis omitted).

80. DONOHUE, *supra* note 2, at 136-38.

81. Sagan, *supra* note 79, at 939. Sagan discussed three factors that vitiate the value of redundancy: common-mode errors, insider threats, and social shirking. *Id.*

less one will know but the more one will be trusted. Since the Snowden disclosures, this paradox has been compounded by a different misunderstanding. Agency oversight officials are charged with preventing waste, fraud, and abuse, which includes illegality. But the bulk metadata collection program ordered by the President, personally approved by the attorney general under guidelines approved by the Justice Department, disclosed to the leaders of both houses of Congress and the chairmen and ranking members of both intelligence committees, and sanctioned in particular cases by more than a dozen federal judges *was not unlawful*. The problem was that the law was arguably secret — not to the Congress but to the public. No oversight system is built to deal with the failure of political judgment that led to that circumstance.[82]

VI. REMEDIES

Professor Donohue and I agree on a number of specific proposals and disagree profoundly on FISA's rationale and constitutional limitations. First, we agree that the 702 database of lawfully collected U.S. Person information should be regulated, though not on how to do it. She asserts that the Constitution requires a Title III warrant before the government can search *its own* database using U.S. Person selectors.[83] This is a novel view, and she provides no support for it. As will be clear in a moment, her proposal is part of an ill-conceived program to re-create the pre-9/11 condition of voluntary ignorance in which the government had to pretend that it did not know things that it did in fact know. If access conditions are going to be imposed, a determination by the Deputy Attorney General that an inquiry was reasonably related to an open federal investigation would suffice to avoid aimless searches of U.S. Person data for an investigatory predicate. In my view, that is the potential evil to be prevented.

Second, we agree that retention limits should apply to known U.S. Person information in the 702 database. I propose a period not to exceed five years.

Third, we both favor relieving FISA judges of some of their other workload as Article III federal district judges during their tenure on the FISC.[84]

Fourth, we agree that the standard for the production of tangible things under FISA should be strengthened. Congress should make it the same as the standard for the obtaining a surveillance order under the act. Both orders involve the same infringement on personal liberty, and it is irrational to think that one kind of

82. *See* Joel Brenner, Forty Years After Church-Pike: What's Different Now?, Henry F. Schorreck Memorial Lecture at NSA, (May 15, 2015) (available at http://joelbrenner.com/forty-years-after-church-pike-whats-different-now-2/).

83. Under the USA Freedom Act of 2015, we require a FISA order before the government can access metadata records held by telecommunications providers, but these are third-party records. USA Freedom Act, Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 (2015).

84. Professor Donohue criticizes the political composition of the FISC as heavily Republican and therefore, in her view, anti-civil liberties. Apart from the dubious connection with political affiliation and libertarian views, she assumes that the number of Democrats on the court reflects the number of Democrats who have been offered the job. One Democratically appointed district judge of my acquaintance turned down the job—too much extra work, he said.

infringement (acquisition of records of past communications) is less serious than the other (acquisition of current communications).

But then Professor Donohue and I part company because, if her basic diagnosis is constitutionally unsound, her favorite remedy could kill the patient. In her judgment, the fundamental problem with the FAA is that it muddled a supposedly clear distinction between foreign intelligence and criminal law. Consequently, she proposes that we build this dichotomy back into law and government operations. This is an appalling proposition, because if we have learned anything since 9/11, it is that the distinction was illusory. The barrier between criminality and foreign intelligence gathering was not done in by a nefarious ideological attack; it collapsed under the weight of the Twin Towers and our inability to track terrorists effectively.[85] Foreign intelligence investigations often, even usually, involve criminal acts,[86] and they often touch our own citizens and territory. Wishful thinking embellished with a different verbal formula will not make these facts go away. Professor Donohue's refusal to acknowledge them then leads her to propose the re-erection of "The Wall"[87]—that is, the hermetical separation of criminal and intelligence investigators that had created a state of self-imposed blind man's bluff between law enforcement and intelligence officials before 9/11, and the abolition of which was essential to our ability to maintain our security. Re-erecting that Wall would mean abolishing or neutering the Justice Department's recently created National Security Division and re-imposing the voluntary ignorance and dysfunctionality by which the government's left hand had no idea what its right was doing. Fortunately, the extreme undesirability of this proposal is matched by the extreme unlikelihood of its being adopted. Neither the country nor the courts are likely ever again to endorse self-imposed ignorance as a national policy.

85. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 270–71 (W.W. Norton & Co. 2004) (2004).

86. *In re* Sealed Case, 310 F.3d 717, 744 (FISA Ct. Rev. 2002) ("[T]he criminal process is often used as part of an integrated effort to counter the malign efforts of a foreign power.").

87. DONOHUE, *supra* note 2, at 27, 150.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

(b) (6)

Fwd: We Need to Prepare for the Future of War

Yll Bajraktari (b) (6)
To: (b) (6)

Tue, Sep 10, 2019 at 11:53 AM

Team,

I highly recommend this article. It has a lot of good materials for us. If we can schedule a meeting with the author that would be fantastic.

Y

Begin forwarded message:

From: Yll Bajraktari (b) (6)
Subject: **Fwd: We Need to Prepare for the Future of War**
Date: September 10, 2019 at 9:59:27 AM EDT
To: (b) (6)

N.S.A. Official: We Need to Prepare for the Future of War

Technology is about to upend our entire national security infrastructure.

By Glenn S. Gerstell

Mr. Gerstell is the general counsel of the National Security Agency.

· Sept. 10, 2019

The National Security Operations Center occupies a large windowless room, bathed in blue light, on the third floor of the National Security Agency's headquarters outside of Washington. For the past 46 years, around the clock

without a single interruption, a team of senior military and intelligence officials has staffed this national security nerve center.

> The center's senior operations officer is surrounded by glowing high-definition monitors showing information about things like Pentagon computer networks, military and civilian air traffic in the Middle East and video feeds from drones in Afghanistan. The officer is authorized to notify the president any time of the day or night of a critical threat.

Just down a staircase outside the operations center is the Defense Special Missile and Aeronautics Center, which keeps track of missile and satellite launches by China, North Korea, Russia, Iran and other countries. If North Korea was ever to launch an intercontinental ballistic missile toward Los Angeles, those keeping watch might have half an hour or more between the time of detection to the time the missile would land at the target. At least in theory, that is enough time to alert the operations center two floors above and alert the military to shoot down the missile.

But these early-warning centers have no ability to issue a warning to the president that would stop a cyberattack that takes down a regional or national power grid or to intercept a hypersonic cruise missile launched from Russia or China. The cyberattack can be detected only upon occurrence, and the hypersonic missile, only seconds or at best minutes before attack. And even if we could detect a missile flying at low altitudes at 20 times the speed of sound, we have no way of stopping it.

The threats of cyberattack and hypersonic missiles are two examples of easily foreseeable challenges to our national security posed by rapidly developing technology. It is by no means certain that we will be able to cope with those two threats, let alone the even more complicated and unknown challenges presented by the general onrush of technology — the digital revolution or so-called Fourth Industrial Revolution — that will be our future for the next few decades.

The digital revolution has urgent and profound implications for our federal national security agencies. It is almost impossible to overstate the challenges. If anything, we run the risk of thinking too conventionally about the future. The short period of time our nation has to prepare for the effects

of this revolution is already upon us, and it could not come at a more perilous and complicated time for the National Security Agency, Central Intelligence Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation and the other components of the intelligence community.

> The immediacy and specificity of the war on terror following the Sept. 11 attacks permitted the intelligence community to reorient itself relatively quickly and effectively from the Cold War and its immediate aftermath. But the intelligence community and its allies who rely on one another for information-sharing must now adapt to adversaries with new capabilities — principally China, Russia, Iran and North Korea, each of which presents different and complex threats — while still not forsaking the counterterrorism mission.

Gearing up to deal with those new adversaries, which do not necessarily present merely conventional military threats, is itself a daunting challenge and one that must be undertaken immediately and for at least the next decade or two. But that is precisely when we must put in place a new foundation for dealing with the even more profound and enduring implications of the digital revolution.

> That revolution will sweep through all aspects of our society so powerfully that our only chance of effectively grappling with its consequences will lie in taking bold steps in the relatively near term. In short, our attention must turn to a far more complex set of threats of multiple dimensions enabled by the digital revolution. While the potential consequences are less catastrophic than nuclear war, they are nonetheless deeply threatening in a range of ways we will have trouble countering.

> There are four key implications of this revolution that policymakers in the national security sector will need to address:

The first is that the unprecedented scale and pace of technological change will outstrip our ability to effectively adapt to it. Second, we will be in a world of ceaseless and pervasive cyberinsecurity and cyberconflict against nation-states, businesses and individuals. Third, the flood of data about human and machine activity will put such extraordinary economic and political power in the hands of the private sector that it will transform the fundamental relationship, at least in the Western world, between government and the private sector. Finally, and perhaps most ominously, the digital revolution has the potential for a pernicious effect on the very legitimacy and thus stability of our governmental and societal structures.

What I offer here is more of a sketch than a finished painting; our national policymakers and the future leaders of those agencies will be responsible for addressing these foreseeable challenges and ultimately finding solutions. While these trends have been extensively discussed in the press, academia and the technical world, there has been far less attention devoted to understanding the combined effect the trends will have on the various agencies that help keep our nation safe. I hope to rectify that shortfall.

We all sense that we are on the cusp of unimaginable technological changes. Cellphones and the internet seem of such manifest utility that we take them for granted, but that is only because they have become so central to our daily lives, not because they have been around forever. Indeed, as we are often reminded, Google started in 1998. YouTube is only 14 years old, and the iPhone is merely 12 years old. The digital revolution thus far is distinguished by its ability to become ubiquitous in our daily personal and commercial lives in an astonishingly rapid time, a time frame that is really without precedent.

Other transformational technologies, such as railroads, electricity, radio, television, automobiles and airplanes, all

took several decades before they reached that comparable level of ubiquity. Society had the time to sort out the norms, rules and laws governing those technologies and the respective roles of government and the private sector. Consider, for example, the lag between the advent of the first useful automobile in the late 19th century and the late 1960s, when safety features became truly significant and mandatory. By contrast, today, just a dozen years after Facebook became a "thing" in our lives, we are forced to grapple with whether and how we should regulate hateful postings and mendacious foreign electoral influence on social media platforms.

Facial recognition technology has in just a handful of years become sufficiently accurate as to be useful and thus more common, but its persistent imperfections have led to a confused spate of lawsuits and statutes seeking to regulate its use. We are far from figuring out its proper role in our society. So the windows for how long it takes for technology to shape society and — more pertinent to this discussion — how long it takes for us to sort out the associated challenges are becoming almost impossibly compressed.

> The time compression for our society and ultimately our national security agencies to deal with these challenges is but one aspect of the problem. The sheer amount of data that will be generated by individual and commercial activities, with the Internet of Things and 5G cellular connectivity, is incomprehensible and will require entirely new ways of rendering that data meaningful to agencies whose mission is to discern threats to national security.

We will need new technologies and systems to capture, analyze and store this data. Obviously, that will require enormous investments by the United States and its allies to upgrade national security and surveillance systems. Will Western liberal democracies, already straining under the

combined demands of decaying civil infrastructure, aging populations, upgrading militaries and so on, be able to afford these investments? Given that there is no specific forcing event to require greater resources, but rather a trend, history suggests that we will appreciate the seriousness of the underinvestment only when a crisis has occurred.

That approach might be a barely acceptable way for our society and government to address social ills and decaying infrastructure, which are slower-moving problems, where with enough resources one might catch up. But the same approach could well be disastrous when addressing rapidly evolving technological matters, especially where national security is at stake. Without such investments, our national security agencies risk becoming profoundly less effective or marginalized.

> While extraordinary levels of new investment will be required to deal with the sheer quantity of data, that alone will not be sufficient. It is futile to believe that we will be able to spend our way to success. Rather, we will need to couple large investment with entirely new ways of approaching how we collect, manage and make sense of this data. One key aspect of any such new approach will be a heavy reliance on machine learning and artificial intelligence. We thought wrestling with the challenges of the Fourth Amendment in addressing electronic surveillance over the past few decades was complicated and contentious, but setting norms for A.I. will surely be even more fraught with difficulty. The stakes are much higher, given that A.I. will be intrinsic to determinations and decisions of almost every aspect of our personal, professional and commercial lives. A.I. opens up the possibility of rendering intelligible for national security purposes that ocean of data. But if misused or even if not thoroughly understood, A.I. can yield nefarious and corrupting results for our society.

Since A.I. is still relatively nascent, our surveillance and analytic resources are not well positioned to deeply understand how adversaries might be using it in the future. The range of novel issues is daunting. For example, we will need to understand how to defend our analytic systems against data poisoning, in which an adversary can feed misinformation to A.I. systems to corrupt or defeat them (such as causing a driverless car to ignore a stop sign).

We will also need to understand the protocols by which future autonomous weapons — drones, tanks, armed robots — will be controlled so that we can defend ourselves. Will the availability of huge numbers of nonhuman war-fighting machines increase the chances of war, as policymakers might be more willing to sacrifice those machines than humans? Or will such machines permit some not-yet-conceived lower threshold of machine-to-machine conflict — whether involving cyber or physical machines — that does not rise to the level of a full-fledged war? Our national security agencies will require new experts and resources to understand the intentions and capabilities of adversaries in this new and developing area.

Understanding the promise and threat of quantum computing will also require vast expansion of our expertise in this extraordinarily sophisticated area. It is true that no one has yet built a functioning quantum computer. Perhaps no one ever will. But it seems more likely than not that before the middle of this century either China or the United States will do so, with extraordinary advantages for whichever nation gets there first.

Unlike the electronic digital computers we have used for over a half century, quantum computers are based on a fundamentally different concept, relying not on simple “on” and “off” states of electricity but on the complex properties of atomic and subatomic particles. One strategic benefit is that quantum computing will enable something that even our current supercomputers cannot

do — crack strong encryption of the type that now protects our commercial financial transactions, our weapons systems and government's secret communications. China's publicly announced 2030 goal is to develop a high-performing quantum computer, which should have that decryption ability. Imagine the havoc that could create. Imagine the overwhelming leverage that the winner would have — such a decryption ability could render the military capabilities of the loser almost irrelevant and its economy overturned.

The analogy of the postwar world in which there was only one nuclear power hints at the type of unilateral dominance that might be possible for the quantum computing victor — but it is not apt here. Even with a nuclear monopoly, there were very real limits on utilizing that capability. But not so with the unilateral capability to decrypt — and thus to understand and perhaps to interfere with or destroy — the entire digital existence of an adversary country.

The strategic advantage here would be for one country to surreptitiously acquire such a capability and maintain it for perhaps several years or more. Other countries would not realize that everything from their weapons systems to financial transactions would be vulnerable during that period; and that would include not only current activity but also the historic, encrypted communications collected and retained by the winner in anticipation of this very capability.

Indeed, one of the strategies yet to be developed involves the paradox of how a country with such capability could exploit it without revealing the capability's existence.

> Moreover, shifting to quantum-resistant algorithms and encryption is theoretical and thus uncertain, but will surely be expensive and a decades-long endeavor.

Over the past several decades, the intelligence community has built up an extraordinary capability to understand the military doctrines and weapons systems of Russia and China. That will still be relevant, but there is now a fundamentally new additional requirement. Under the best of circumstances, it would take many years to develop comparable levels of expertise about those countries' use of A.I., quantum computing or other novel technologies. Such technologies range from hypersonic missiles, which Russia and China are racing to develop — with the potential to upend the entire global balance of power — to synthetic biology and genetic manipulation, with the potential to create new biological weapons or immunities. Our national security sector does not have an extensive history of marrying intelligence insight and analysis with deep technical expertise across a wide range of scientific disciplines.

That might not, however, be the limiting factor.

> It is by no means assured that our national security sector will be able to attract on a sufficient scale the scarce engineering, mathematical and scientific talent that would supply the necessary expertise. That challenge will require investment, enlightened strategic management and an innovative approach to luring a different type of expert out of the private sector into government. Meeting this challenge will require a greater reliance in general on the private sector, since government alone does not possess the requisite expertise. A large portion of the

intelligence community's experts on the military capabilities and plans of Russia and China joined government during the Reagan administration; other experts on counterterrorism and new technology burnished their technical skills following the Sept. 11 attacks. Many of those experts are nearing retirement or have already left to join an attractive private sector. With millennials believing that technology in the private sector now allows them to help change the world — previously the idea of a mission had been largely the province of public service — it is not clear that the intelligence community will be able to attract and retain the necessary talent needed to make sense of how our adversaries will make use of the new technology.

In short, while important work has been done in examining and laying the foundations for the critical role new technologies will play in national security, much more needs to be done. We must ask whether our defense and national security establishments are in a position — financial and technical — to succeed in these critical technologies that could either solidify our continued position as the leading global power or reduce us to a clearly subordinate role. We are talking about national initiatives that collectively will dwarf the effort to put a man on the moon.

Bluntly put, there are few signs that our society overall and our political leaders have fully embraced the challenge or appreciate the risks of failure.

All of this technological innovation will surely bring significant societal benefits, perhaps most notably in the area of health care and genetic engineering, but it will also increase — to use a hackneyed but useful term — the "attack surface" for cyber mischief. This takes us to the second

implication of the digital revolution: We must prepare for a world of incessant, relentless and omnipresent cyberconflict — in not only our national security and defense systems (where we are already used to that conflict) but also, more significantly, every aspect of our daily and commercial lives.

> The sensors, systems, networks, algorithms and machines that will empower our new lives — whether health care implants, driverless cars, pilotless aircraft or food safety protections — will all be part of the Internet of Things. One consequence is that the current division between cyberdefense (think firewalls, penetration testing and cyberhygiene) and supply-chain risk management (think of the assessment of equipment manufacturing, component assurance and availability and surveillance concerns in equipment) will be eliminated, with everyone concerned with the holistic sanctity of equipment and software to achieve the well-recognized triad of availability, security and integrity.

The 40-odd nation-states that today have offensive cybercapabilities will seem a quaint historic artifact when sophisticated tools for cybermischief are in the hands of not only every nation-state but also common criminals around the globe. While most nation-states might be careful to limit their cybereffects to economic theft and espionage, pre-battle positioning of beacons and other malware, mischievous interference with elections and public opinion — all below levels that cause significant physical damage to infrastructure or physical harm to humans, and thus below at least what we currently think of as the threshold for an act of war — there is no guarantee that all nations will exercise such care nor that criminals would be deterred. Consider how North Korea seems able to operate with relative impunity in cyberspace, knowing that it is unlikely to provoke an armed

attack partly because of its perceived willingness to retaliate in ways that would impose unacceptable consequences on Western society. Multiply that dynamic across a dozen or more countries or international terrorists or criminal gangs and we are now faced with an entirely different national security threat.

To be sure, our nation has set forth its cyberstrategies and continues to refine its offensive and defensive doctrines in cyberspace, but nearly every expert would concede more needs to be done. The question is whether we will be able to do it in time, since the threat is coming at us with the speed and force of a tsunami.

> The simple fact of the matter is that no nation has yet devised an effective solution to the conundrum of how to respond in a definitive and dispositive way to another nation-state's malicious cyberactivity. Whole-of-government approaches — economic sanctions, judicial prosecutions and offensive cyberresponse below the war threshold — while essential and appropriate, have not been enough to stop cybermalevolence. In short, the problem is going to get worse before it gets better.

In all probability, it will get better not because we develop more effective deterrents (although threats of cyberretaliation and imposition of other burdens clearly do play a key role here, at least with other nation-states) but because we develop greater resilience and more impervious defenses — and the full realization of that may be a decade away.

In the meantime, our national security agencies will be confronted with the political imperatives in our democracies of responding (at least in some way) to cyberthreats. Among other things, our citizens and businesses will have to accept that cybermalevolence is a persistent threat, not a war to be won or a disease to be cured. Moreover, since the threat is ignorant of sovereign boundaries, agencies charged with cyberprotection will be required to work with many others around the globe, perhaps including those of adversary or competitor nations, creating new complexities.

At a minimum, the worldwide cyberthreat will put a premium on trusted relations among the Five Eyes (the United States, Britain, Canada, Australia and New Zealand) and other like-minded nations, to facilitate working together to counteract malevolent activity that can span the globe in seconds. Even among such long-term, cohesive arrangements as the Five Eyes alliance, unity of effort in cyberspace is not assured, as witnessed recently by differing approaches to the risks posed by Huawei equipment in 5G networks.

The third implication of the digital revolution is that the balance between government and the private sector will be altered in a profound way. That in turn is the inescapable product of three factors: cybervulnerability affecting every element of the private sector (no longer are targets arguably limited to military assets), the general flood of data unleashed by the digital revolution that will be created in the hands of private enterprise and a response to a rising China whose strategic technology goals pose a unique threat that directly implicates the private sector.

Even without considering the challenges presented by China, there are at least two, related manifestations of how the government-private sector balance has changed and will change. First, the government no longer possesses the lead in complex technology, at least in many areas relevant to national security. Arguably, the most powerful computing and sophisticated algorithm development now occurs not in the Pentagon or the N.S.A. but in university research labs and in the Googles and Amazons of the commercial world. (To be sure, the government still maintains its superiority in important areas ranging from nuclear energy to cryptography.) Even apart from the issue of which sector has the technological edge, there is the simple fact that the digital revolution has brought astonishing capabilities to anyone who has a smartphone, who can now download a facial recognition

app, a malicious cybertool or some other capability that formerly was the exclusive province of government.

Second, the private sector will have many more times the quantity of data about individuals and commercial activity than governments could ever obtain. The larger antivirus vendors, with their sensors connected to their global corporate clients, already know more at any given moment about the state of networks around the world than does any government agency. Businesses in the services, retailing, industrial and other sectors will have more global sensors and applications detecting cybertraffic, collecting behavioral patterns, amassing personal data and so on, than even the most surveillance-oriented nation could ever hope to have. The fact that private satellite imagery companies have displaced the monopoly that the National Geospatial-Intelligence Agency used to have is merely a harbinger of how the private sector will be the collector and repository of key information about our locations, our consumption patterns, our communications — in short, about everything.

As the owners of physical infrastructure learned following the Sept. 11 terrorist attacks, when our everyday lives rely on the security of assets and services held in the private sector, commercial owners will be expected to take steps to protect society. We are clearly witnessing the same imbuing of social responsibility into how the digital revolution's data will be handled. Personal data needs to be safeguarded so that it does not fall into the wrong hands, it needs to be made accurate so that incorrect results are not generated from its use, and it needs to be

used in ways that do not violate our notions of privacy and proper use. Those are not duties originating within the commercial world but will be increasingly imposed by society.

As for the safeguarding, many would argue that governments cannot and should not be relied on to prevent and defend against every cyberthreat to the private sector, even from a nation-state; such threats are not the same as an armed attack. But that leaves the private sector frustrated and underdefended — hacking back is often impossible and generally illegal.

National security agencies will need to defuse that frustration and find an effective path for collaboration with the private sector to mitigate cyberthreats. The only practical solution is for the private sector to assume a greater burden in this area, but with the active support of the national security agencies. We are still struggling to find an effective solution to the competing desires for the private sector to obtain classified information about cyberthreats and for government to obtain detailed information about cyberintrusions into corporate networks. Both sides have legitimate reasons to keep their information secret. But ultimately we all realize that will not yield an effective outcome. Attribution solutions will require the private sector to be more forthcoming about network breaches. Indeed, the private sector should have a greater responsibility to collect, analyze and retain all this new data and to make it available with appropriate safeguards to the government for national security purposes. But even safeguards will not completely allay a variety of privacy and liability concerns.

Until recently, at least in the United States, our notions of privacy have been rooted in the Fourth Amendment's delineation of the federal government's powers vis-à-vis the individual citizen. But what do our notions of privacy mean anymore when Amazon, Google, Apple, Microsoft, Facebook and so on already know so much about you? We now see increasing pressure in Congress to regulate in this area. To be sure, this article is not advocating any particular approach (much less suggesting greater surveillance powers), but it is hard to escape the conclusion that we will need to recalibrate the balance in this area of data privacy between the government and the private sector.

National security agencies should affirmatively contribute to the public discourse about this recalibration. The challenge for those agencies will be to find the right approach to working with the private sector to obtain the data needed to fulfill their vital missions in a manner that fits our values and cultures.

Of course, there is another path, and it is the one taken by authoritarian regimes around the world. China's approach is to have all that data reside in the central government, in a vast databank of personally identifying information about its citizens, from iris and facial recognition to DNA data. That is antithetical to our values.

> But it is equally true that to keep our society safe, those charged with that mission will need some access to that data. Absent some satisfactory calibration, our national security agencies run the risk of being marginalized and ultimately irrelevant and ineffectual, with grave consequences for national security.

> Eschewing the approach taken by authoritarian regimes to data collection and usage by no means reveals the proper path to be taken, as any decision would be deeply

linked to the historic roles of government and the private sector in each country. The approach in Western Europe, with close cooperation between public and private sectors, might seem inappropriate if not impossible in America.

For two examples, consider the integrated cybercenters in Britain and the level of government involvement in private sector data usage under the European Union's General Data Protection Regulation. Would the American business community accept that model, and would our national politics permit its adoption? Paradoxically, the global cyberthreat and the overall challenges presented by the digital revolution may propel national security agencies of many countries to work together, but they may find closer cooperation difficult in practice as the balance between public and private sectors will vary greatly from nation to nation.

Finally, our nation will have no choice but to harness the collective capabilities of the government and the private sector to address the combined technologic and economic threats posed by China. For the first time since the United States became a global power, it must now confront an adversary that presents not merely a political or military threat but also an existential economic one. But in the latter area, the playing field is not level, as China advances its national strategic goals through a unified effort harnessing its government and its business sectors (the latter being a mix of private and state-sponsored endeavors) — while our strategic goals are seen as the responsibility of the federal government, with our private sector largely free to pursue its capitalist interests as it sees fit.

The almost inescapable fact that China's economy will surpass ours in size has obvious national security implications. But two circumstances present special challenges for our national security community. The obvious one is that China continues to seek economic and military superiority through cybertheft from our government, defense industrial base and academia. The second is that our national security agencies for the first time must amass the talent and systems to understand not simply a military challenge but also challenges across a broad range of technology and global finance issues. The capacity for such understanding currently resides principally in the private sector and our universities, not the federal government.

Both of those circumstances will force the government and private sector to work together in unprecedented coordinated and mutually supportive ways if we are to rise to the challenges posed by China. That will require changes in not only attitudes (on both sides) but also laws to permit greater collaboration.

The digital revolution is at least partly responsible for another disruptive effect on the relationship between governments and the private sector, namely the almost complete globalization of economic forces. That capital is now a global commodity shows the relative shortcomings of a nationalistic approach to protect vital assets. Most Western democracies have some rules to regulate foreign investment in critical industrial sectors. In the United States, the Chinese have figured out that it is easy to sidestep the strictures of the Committee on Foreign Investment in the United States, which limits foreign investment in nationally sensitive industries, simply by investing in start-ups and other ventures that have access or insight into critical technologies or by working in university research labs to the same end. This may well be another factor weakening the role of nation-states in providing security and tilting the balance of power toward the private sector, which is in a better position to police unwanted investments and intellectual property theft.

As if all this is not disconcerting enough, the fourth implication is that the internet can have a pernicious effect on our democracies, where adversaries can take advantage of our freedoms and interfere with our societal and government institutions. The painfully obvious fact is that the internet affords everyone a communications capability. In the absence of a commonly accepted authority — whether it be a trusted government or a curated news source — the internet permits lies and evil to be spread with almost no check.

> A world in which effective deception in almost every venue and media outlet is possible vastly complicates the duties of government and societal institutions. Even if a nation were to control its own citizens' activities, information (whether accurate or not) knows no national boundaries.

We all recognize this decentralizing and delegitimizing force, and there is no need to elaborate on it here. Worth appreciating in this context, however, is that governmental agencies with a national security mission are going to find it vastly more difficult to maintain the necessary trust, respect and support of a democratic populace in this environment — jeopardizing not only their ability to obtain resources from society but also in the end their very mission.

Indeed, the state of affairs of fundamental uncertainty and doubt that will be facilitated by the misuse of digital technology may well make it more difficult to maintain foreign alliances (which, after all, are based on trust) — precisely at a time, paradoxically, when global cooperation is required to counter malicious activity. In short, and perhaps most critical to appreciate, the fourth implication of the digital revolution is that it will make dealing with the first three implications all the more problematic.

Putting these four implications together — coping with unprecedented technological change, adapting to a world of unceasing cyberconflict, navigating concepts of privacy and the power that comes with access to big data in the hands of the private sector, and countering the insidious and pernicious effects of the delegitimization afforded by the malign use of the internet — yields at least two imperatives, both of which are transformational.

> The first imperative is that our national security agencies must quickly accept this forthcoming reality and embrace

the need for significant changes to address these challenges. This will have to be done in short order, since the digital revolution's pace will soon outstrip our ability to deal with it, and it will have to be done at a time when our national security agencies are confronted with complex new geopolitical threats.

Much of what needs to be done is easy to see — developing the requisite new technologies and attracting and retaining the expertise needed for that forthcoming reality. What is difficult is executing the solution to those challenges, most notably including whether our nation has the resources and political will to effect that solution. The roughly $60 billion our nation spends annually on the intelligence community might have to be significantly increased during a time of intense competition over the federal budget. Even if the amount is indeed so increased, spending additional vast sums to meet the challenges in an effective way will be a daunting undertaking. Fortunately, the same digital revolution that presents these novel challenges also sometimes provides the new tools (A.I., for example) to deal with them.

The second imperative is we must adapt to the unavoidable conclusion that the fundamental relationship between government and the private sector will be greatly altered. The national security agencies must have a vital role in reshaping that balance if they are to succeed in their mission to protect our democracy and keep our citizens safe. While there will be good reasons to increase the resources devoted to the intelligence community, other factors will suggest that an increasing portion of the mission should be handled by the private sector. In short,

addressing the challenges will not necessarily mean that the national security sector will become massively large, with the associated risks of inefficiency, insufficient coordination and excessively intrusive surveillance and data retention.

A smarter approach would be to recognize that as the capabilities of the private sector increase, the scope of activities of the national security agencies could become significantly more focused, undertaking only those activities in which government either has a recognized advantage or must be the only actor. A greater burden would then be borne by the private sector.

For example, our society could consider greater coordination between government and the private sector in advancing national security strategic goals (such as development of quantum computing capabilities), specific requirements for the private sector to share (with appropriate safeguards) proprietary data and technology with the government where directly relevant to national security, or a duty to notify government of the details of cyberincidents. Perhaps we should rekindle the discussion over a national service obligation to help supply technical expertise to the government across a broad range of fields, or otherwise create some arrangement to make such expertise available to government (rather than the current model in which the private sector often lures away government-trained talent). The point here is not to advocate for any of these, simply to say our policymakers need to be examining alternatives if we are to close the forthcoming technology gap.

Although I have sketched out some of the more troublesome implications of the digital revolution for the national security sector, it is not in the spirit of forecasting doom, but rather to sound an alarm.

Our innovative and entrepreneurial society affords us a unique advantage in dealing with those implications. Moreover, no adversary should ever underestimate the extraordinary capabilities of our armed forces and intelligence community — like those keeping watch at the

National Security Operations Center. Their prowess and resilience will be key in addressing future challenges. But it would be a mistake to rely on these strengths alone.

Surmounting the transformational challenges posed by this Fourth Industrial Revolution will require not merely resources and creativity from both the public and private sectors but also, and more critically, a level of concerted national political will that may be made all the more difficult to achieve by the very attributes of the digital revolution rushing toward us.

Mr. Gerstell is the general counsel of the National Security Agency and previously served as a member of the president's National Infrastructure Advisory Council.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

(b) (6)

The US Air Force is enlisting MIT to sharpen its AI

1 message

The Algorithm from MIT Tech Review <newsletters@technologyreview.com> Tue, May 21, 2019 at 12:27 PM
Reply-To: newsletters@technologyreview.com
To: (b) (6)

The Algorithm

Artificial intelligence, demystified

Diagnosis by algorithm

05.21.19

Hello Algorithm readers,

At the request of our readers, we now have an informal archive of all of our issues here. This week's issue begins with two stories from senior AI editor Will Knight on the use of machine learning in cancer detection and in the US air force, plus another story on Amazon's face recognition platform.

google cancer

AI could detect lung cancer faster and more reliably. Lung cancer killed more than 160,000 people in the United States in 2018, making it the leading

cause of cancer death. And while computed tomography (CT) scans can be a life-saving part of cancer screening, they are also often unreliable.

On Monday, Google published a new paper in *Nature* showing how machine learning could change that. Researchers trained and tested a deep-learning algorithm with more than 42,000 CT scans to detect malignant lung nodules. The resulting model turned up 11% fewer false positives and 5% fewer false negatives than human radiologists. The work still needs to be validated on larger patient populations.

The paper comes amid a growing interest in using AI to catch many types of cancer. Researchers have shown how machine learning can also be used to spot both breast cancer and skin cancer, for instance. While these studies are exciting, they should be treated as small advances. Applying AI in healthcare remains challenging for privacy reasons. Real-world data sets are also rarely as perfect as those used in research studies. **Read more here.**

aircraft

The US Air Force enlists MIT. The US Air Force is one of the most advanced fighting forces in the world—and yet it's worried about losing that edge in the age of AI.

To address that, it announced a collaboration with MIT yesterday that will focus on developing and harnessing the technology. The Air Force Artificial Intelligence Incubator will advance uses of AI "for the public good," meaning applications relevant to the humanitarian work done by the Air Force and not directly connected to the development of weapons. That caveat might be key in

preventing a backlash from students and the community—although that's far from certain.

Machine learning could optimize many mundane things in the military, from payroll to logistics. It will also be vital to a critical aspect of missions: gathering intelligence and extracting useful insights. This is far broader than the development of autonomous weapons—a topic that often comes up when people think about the military applications of AI.

In February, the Pentagon posted an unclassified document (pdf) outlining its plan for embracing artificial intelligence. The document made it clear that the technology is crucial to the military's preeminence. Military adoption of AI in other countries, especially Russia and China, is also a key driver. Will spoke to US Air Force Secretary Heather Wilson about the new incubator. **Read more here.**

Amazon's shareholders vote on face recognition. On Wednesday, Amazon's shareholders are gathering in Seattle to determine whether the tech giant has gone too far in infringing civil liberties by selling face recognition technology. They will vote on two proposed measures: whether to prohibit the sale of Amazon Rekognition, the company's face recognition platform; and whether to commission an independent report investigating the extent to which Rekognition may threaten civil, human, and privacy rights—and what the resulting bad press might do to the company's finances.

Even if they pass, the proposals would be non-binding, meaning they wouldn't require Amazon to take action. But they will pile onto the mounting scrutiny that Rekognition has received, including from civil liberties groups, AI researchers, and the company's own employees. The proposals also come a week after San Francisco became the first city to ban the government's use of face recognition, triggering a wave of other cities to consider like-minded action.

Despite growing public unease around its use, Amazon continues to sell its service to law enforcement agencies. "We have not seen law enforcement agencies use Amazon Rekognition to infringe on citizens' civil liberties," the firm said in a statement.

TR ARCHIVE

My piece on why making face recognition less biased doesn't make it less scary: "Even the fairest and most accurate systems can

still be used to infringe on people's civil liberties. Last year, a Daily Beast investigation found that Amazon was actively pitching its facial surveillance platform to US Immigration and Customs Enforcement, better known as ICE, to aid its crackdown on migrant communities. An Intercept investigation also found that IBM developed the ability to identify the ethnicity of faces as part of a long-term partnership with the New York Police Department. This technology was then deployed in public surveillance cameras for testing, without the knowledge of city residents." **Read more here.**

Augmented reality is not just a fun tool – it's being used to build spacecrafts and train workforces.

How can your business leverage emerging technology for the future of work?

IMAGES OF THE AUDIO SPECTROGRAMS FOR THE INPUT LANGUAGE AND THE OUTPUT TRANSLATION FOR A TRADITIONAL AUTOMATED SYSTEM VERSUS TRANSLATOTRON.

Cómo estás? One day you might sound like you can speak Spanish even if you don't. In a new paper, Google prototyped an automated translation system that translates speech from one language to another while retaining the voice and tone of the original speaker. Traditional translational systems convert audio into text, translate the text, and then resynthesize the audio, losing the characteristics of the original voice along the way. In contrast, the new system converts audio input directly to audio output without any intermediary steps.

The Translatotron, as it's known, has three components, all of which look at the speaker's audio spectrogram—a visual snapshot of the frequencies used when the sound is playing, often called a voiceprint. The first component uses a neural network trained to map the audio spectrogram in the input language to the audio spectrogram in the output language. The second converts the spectrogram into an audio wave that can be played. The third component can then layer the original speaker's vocal characteristics back into the final audio output.

Not only does this approach produce more nuanced translations by retaining important nonverbal cues, but in theory, it should also minimize translation error because it reduces the task to fewer steps. **Listen to audio examples here.**

BITS AND BYTES

Facebook's AI executive faces a Herculean task
He admits that the tech giant will never successfully eliminate all toxic content. (NYT)
+ Using AI to screen for dangerous videos is still a long way off (Bloomberg)

The AI chip boom is challenging Nvidia
The gold rush to make custom-made silicon for deep learning is reshaping the global market. (WSJ)

Facebook wants to use robots to advance AI and AI to advance robots
It's new robotics lab aspires to bridge the digital and physical worlds. (TR)

China shouldn't have openly declared its AI ambitions
The move has alarmed the US and the rest of the world. (SCMP)

New apps are helping people learn to flirt and sext
One uses machine learning to evaluate people's texts and then coaches them on how to be more engaging. (NYT)

Uber and Lyft drivers have learned to manipulate the apps' prices
Every night at Reagan National Airport, they simultaneously turn off their rideshare apps for a few minutes to trick the algorithm into creating an artificial price surge. (WJLA)

QUOTABLE

It won't be fixed tomorrow. But I do not want to have this conversation again six months from now. We can do a much, much better job of catching this.

—A tearful Mike Schroepfer, Facebook's chief technology officer, on the devastating failure of AI to prevent the livestream of the Christchurch shooting


Karen Hao

Hello! You made it to the bottom. Now that you're here, fancy sending us some feedback? You can also follow me for more AI content and whimsy at @_KarenHao, and share this issue of the newsletter here.

Was this forwarded to you, and you'd like to see more?

Sign up for free

View this in a browser

You received this newsletter because you subscribed with the email address: (b) (6)

edit preferences | unsubscribe | follow us

MIT Technology Review
One Main Street
Cambridge, MA 02142

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

(b) (6)

ACLU/Ben Wizner

1 message

(b) (6)
To: (b) (6)

Wed, Sep 11, 2019 at 1:01 PM

https://www.aclu.org/blog/privacy-technology/surveillance-technologies/artificial-intelligence-any-cost-recipe-tyranny

NSCAI list of organizations consulted between March 2019 and October 2019

Aerospace Industry Association
AFWERX
AI Sustainable Development Group
Air Force Research Lab
Algorithmic Warfare Cross Functional Team, DoD
Amazon
American Civil Liberties Union
American Psychological Association
Anduril
Arizona State University
Army Futures Command
Army Research Lab
Army War College
Asia America Multi Technology Association
Association for the Advancement of AI
Atlantic Council
Australian Strategic Policy Institute
Battery Innovation Center
Booz Allen Hamilton
Brookings Institution
Bureau of Industry & Security
C3IOT
California Polytechnic State University
Carnegie Endowment for International Peace
Carnegie Mellon University
Center for a New American Security
Center for Democracy & Technology
Center for Naval Analysis
Centre for Effective Altruism
Central Intelligence Agency
Cisco Systems
Coding it Forward
Computer Science & Telecommunications Board
Computing Research Association
Cybersecurity & Infrastructure Security Agency
Cyberspace Solarium Commission
Data & Society
Defense Advanced Research Projects Agency
Defense Innovation Board
Defense Innovation Unit
Defense Intelligence Agency
Deloitte
Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of State
Department of the Air Force
Department of the Army
Department of the Navy
Department of the Treasury
Draper Laboratory
Duke University
Electronic Frontier Foundation
Elsevier
Embassy of Australia
Embassy of Canada
Embassy of the European Union
Embassy of France
Embassy of Japan
Embassy of the United Kingdom
Energy Systems Network
Ethical Intelligence Consulting
Eurasia Group
Federal Bureau of Investigation
Federation of American Scientists
Franklin Templeton Investments
Future of Privacy Forum
General Dynamics
Georgetown University
Google
Govini
Harvard University
Harvard-MIT Ethics & Governance of AI Initiative
Heritage Foundation
Howard University
Human Rights Watch for the Campaign to Stop Killer Robots
IBM
Intelligence Advanced Research Projects Activity
In-Q-Tel
Indiana Economic Development Corporation
Indiana General Assembly
Indiana Innovation Institute
Indiana Office of Defense Innovation
Indiana University
Institute for Defense Analyses
International Committee of the Red Cross
Johns Hopkins University
John Hopkins University Applied Physics Lab
Joint Artificial Intelligence Center
The Joint Staff, DoD
Kessel Run
Lockheed Martin
Marine Corps
Marine Corps Warfighting Laboratory
Massachusetts Institute of Technology

McKinsey
Microsoft
MIT Lincoln Laboratory
National Commission on Military, National & Public Service
National Defense University
National Geospatial-Intelligence Agency
National Institute of Standards & Technology
National Reconnaissance Office
National Science Foundation
National Security Agency
National Security Council
National Security Innovation Network
Naval Sea Systems Command
Naval Surface Warfare Center - Crane
Naval Undersea Warfare Center Division – Keyport
Navy Digital Warfare Office
Networking & Information Technology Research & Development Program
New York University
Northrop Grumman
Notre Dame University
Odlum Strategies, LLC
Office of Civil Liberties, Privacy & Transparency. ODNI
Office for Civil Rights & Civil Liberties, DHS
Office of Commercial & Economic Analysis, DoD
Office of the Director of National Intelligence
Office of Management and Budget
Office of Naval Research
Office of Personnel Management
Office of the Secretary of Defense
Office of Science & Technology, DHS
Office of Science & Technology Policy, The White House
OpenAI
Pacific Northwest National Lab
Palantir Technologies
Partnership for Public Service
Partnership on AI
Paulson Institute
Presidential Innovation Fellows
Privacy Office, DHS
Primer.ai
Privacy & Civil Liberties Oversight Board
Purdue University
Radius Indiana
RAND
Raytheon
Reagan Institute
SAP National Security Services
Schmidt Futures
Semiconductor Industry Association
SensorHound
Shield AI
SIMBA Chain
Singularity University
SoftBank
Software Engineering Institute
SOSI
Stanford University
Tech Inquiry
The Engine
The Technical Cooperation Partnership
Tufts University
U.S. House of Representatives
U.S. International Trade Commission
U.S. Senate
U.S. Special Operations Command
U.S.-China Economic & Security Review Commission
United States Air Force Academy
United States Military Academy
United States Naval Academy
United States Naval War College
University of California System
University of California, Berkeley
University of Chicago
University of Illinois at Urbana-Champaign
University of Oxford
University of Pennsylvania
University of Southern California
University of Southern Indiana
University of Washington
University of Washington Applied Physics Lab
Xnor
Yale University