Error 404 – Trust Not Found

A European Survey on Digital (Dis)trust

Munich Security Brief
March 2021
Authors

Simon Pfeiffer
is a Policy Advisor at the Munich Security Conference.

Randolf Carr
is a Policy Advisor at the Munich Security Conference.
Summary

A joint tech agenda is one of the key priorities of the transatlantic partnership. An exclusive survey on behalf of the Munich Security Conference (MSC) finds that to deliver on this goal, European leaders need to address a high level of digital distrust in Europe – amongst Europeans, but especially vis-à-vis the United States.

At the MSC Special Edition in Munich on February 19, world leaders including US President Joe Biden, German Chancellor Angela Merkel, French President Emmanuel Macron and British Prime Minister Boris Johnson gathered to send a strong signal of transatlantic renewal. In the wake of a joint agenda to “build back better,” cooperation on technology has emerged as one of the key priorities.

However, there is a substantial hurdle: As an exclusive survey conducted in six European countries in early 2021 shows, Europeans are deeply concerned about their security and that of their personal data online. Most respondents think their governments are not doing enough to protect them in the digital world and worry about dependencies on foreign suppliers of digital technologies. The survey shows that trust in digital technology does not extend far beyond national borders: Europeans are skeptical of governments and companies from other European countries. This “digital distrust” is only exacerbated when looking across the Atlantic. Most respondents believe data stored by US entities is not secure and find their countries to be too dependent on US technology imports. Vis-à-vis China, such concerns are even more pronounced. European leaders need to address this “digital distrust” – at home and toward the United States. Otherwise, it might threaten progress on the transatlantic tech agenda and put a dent into ambitions of the European Union as a “regulatory superpower.” But there is a silver lining: European leaders have a clear mandate to act. There is an opportunity to make substantial progress toward a shared democratic technology governance.

This Munich Security Brief serves as a discussion starter for working towards transatlantic digital trust. It is part of the MSC’s “Road to Munich 2021” campaign, which aims to highlight key items on the agenda for renewing transatlantic cooperation.
Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust

In 2020, the Munich Security Conference chose the motto of “Westlessness” for its annual conference. The developments over the last year have vindicated our diagnosis: The severity of the Covid-19 pandemic in North America and Europe as well as the absence of meaningful transatlantic cooperation to contain the pandemic and its consequences, the continued erosion of liberal-democratic norms in many Western countries, and a general sense of decreasing global influence all substantiated the analysis of a weakening West – “at home” and in the world. Yet, the election of Joe Biden as US president has been the starting point for efforts to overcome the state of “Westlessness” on both sides of the Atlantic: At the MSC Special Edition on February 19, which was broadcast live to millions of viewers around the world, President Biden and European leaders jointly expressed their ambitions for a renewal of the transatlantic partnership. To move forward, the partners now need to use the momentum and deliver concrete results.

A major issue on the agenda is cooperation on technology. The list of pressing concerns, further heightened in urgency due to the acceleration of digitalization in the context of the Covid-19 pandemic, is long and cuts through all areas of transatlantic politics: From the digital tax to competition policy, privacy, and the sharing of personal data, technology issues are front and center. Discussions about secure supply chains, most prominently regarding 5G equipment, are another major bone of contention. In the defense sector, data interoperability and data sharing are now critical, as recent defense strategies emphasize the necessity of substantially increasing investment in emerging technologies. The prevalence of an “age of perpetual cyberconflict” was showcased once more by the recent SolarWinds and Microsoft Exchange hacking incidents, allegedly perpetrated by Russia and China, respectively. All of these issues have taken center stage as technology has become an arena for geopolitical competition. In particular, the increasingly fierce competition between the United States and China has put a spotlight on power and control in the digital sphere.
Against that background, setting future standards for the governance of the internet, data, and digital technology has been a long-held ambition for the transatlantic partners. With the election of Joe Biden and the commitment of Europe and the United States to renew the transatlantic partnership, a window of opportunity has now opened to address these issues. Demonstrating the ability to foster digital trust among their citizens could act as a powerful selling point for the liberal-democratic model. The world is in a competition for the best approach to harnessing technology and the digital economy. If the world’s democracies can agree on common rules, this would go a long way toward promoting a global digital order reflecting liberal-democratic values.

Scorched Earth: European Digital Distrust

So is the transatlantic tech agenda set up for success? The list of policy issues on which the EU and the United States are far apart is almost as long as the list of priorities itself. Moreover, the last four years have seen European digital sovereignty endorsed as a priority of EU tech policy at the highest level, a development that has elicited concern from across the Atlantic. European policy-makers have claimed that digital sovereignty is not defined “against” anyone else. But these debates revealed that “from a European point of view, the United States is the primary ‘other’ that Europe measures itself against on technology.” The result has been little headway being made on technology cooperation over the last years – despite the multiplicity of critical issues that the transatlantic partners must address and resolve together.

These hurdles can be overcome: Arguably, the perception gap on questions from competition policy to 5G is closing. The European Commission proposed an EU-US agenda with proposals such as a “trade and technology council,” a “dialogue on the responsibility of online platforms,” or common solutions to antitrust enforcement and taxation in the digital sphere shortly after the election of Joe Biden. At the virtual gathering in Munich, Commission President Ursula von der Leyen extended an offer of cooperation to the United States, repeatedly emphasizing shared values and goals – a clear departure from the strong language of European sovereignty that had dominated the previous four years and has resonated with the European publics.
Given indications of willingness to cooperate from both Brussels and Washington, the time is ripe to move the ball forward. To help open the transatlantic conversation and to lay the groundwork by shedding light on the status quo, the MSC commissioned an exclusive survey on this pressing issue. Across six European countries, citizens were asked about their concerns and perspectives regarding technology with a focus on questions of security, trust, and fear of dependency. Whether trust is present, ultimately, is in the eyes of the user. The survey reveals that the past decade has changed how Europeans perceive the digital world: Their perspective is dominated by concerns about their security and that of their personal data. Instead of embracing the potential for a common governance, they fear data theft, fraud, and increasing national dependency on untrustworthy foreign suppliers, both European and, to a greater degree, suppliers further abroad.

**Insecure Network: The Internet Is a Dangerous Place**

Over the last five years, European citizens have become significantly more careful when acting online (see Figure 1). This concerns both personal information and the information they interact with: Compared to five years ago, two thirds of respondents have become more cautious regarding the reliability of information they find online; 60 percent are now more cautious with respect to the security of their devices and accounts. This development of growing caution follows a broader trend of decreasing trust in the technology sector and skepticism about the veracity of information across the media landscape in recent years.

On behalf of the Munich Security Conference, Kekst CNC conducted a representative survey among the general population in France, Germany, Italy, Poland, Sweden, and the United Kingdom for this report. For this survey, a total of 6,039 respondents were interviewed. The results were quota-adjusted and weighted to be nationally representative of each country surveyed. The survey was conducted in January 2021, using an online questionnaire.
Compared to five years ago, are you more or less cautious regarding...

"Whether from our streets or from our screens, we should be able to do shopping in a safe manner. Whether we turn pages or scroll down, we should be able to choose and trust the news that we read. And of course, what is illegal offline is equally illegal online."  
Margrethe Vestager, European Commissioner for Competition and Executive Vice President of the European Commission for A Europe Fit for the Digital Age, Brussels, December 15, 2020

Our survey also reveals how fundamentally skeptical Europeans are about the security of their personal data. Eight years after the Snowden revelations let fears about the misuse of private data skyrocket, Europeans across all surveyed markets substantially doubt the ability, the willingness, or both of most institutions outside of their country to protect their personal information (see Figure 2). The private companies with which citizens interact – for example, their employers, service providers, and their national digital sector – are trusted most. In net terms, these companies were ranked as more trustworthy than national governments in all countries, except for Sweden. This may reflect prominent attacks against government institutions such as the hack against the German parliament in 2015, for which the EU levied sanctions on two Russian officials in 2020.28
How confident are you in the following organizations’ ability and willingness to protect your personal data?

- Very confident / confident
- Not confident / not confident at all

<table>
<thead>
<tr>
<th>Organization</th>
<th>Very Confident</th>
<th>Not Confident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your employer</td>
<td>40%</td>
<td>17%</td>
</tr>
<tr>
<td>Your internet service provider</td>
<td>40%</td>
<td>20%</td>
</tr>
<tr>
<td>Your mobile phone network</td>
<td>36%</td>
<td>22%</td>
</tr>
<tr>
<td>Tech companies in your country</td>
<td>33%</td>
<td>23%</td>
</tr>
<tr>
<td>Your national government</td>
<td>33%</td>
<td>31%</td>
</tr>
<tr>
<td>European companies</td>
<td>23%</td>
<td>31%</td>
</tr>
<tr>
<td>Other European governments</td>
<td>19%</td>
<td>38%</td>
</tr>
<tr>
<td>US tech companies</td>
<td>18%</td>
<td>46%</td>
</tr>
<tr>
<td>The US government</td>
<td>13%</td>
<td>55%</td>
</tr>
<tr>
<td>Chinese tech companies</td>
<td>10%</td>
<td>64%</td>
</tr>
<tr>
<td>The Chinese government</td>
<td>9%</td>
<td>70%</td>
</tr>
</tbody>
</table>

Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.
Excluding “don’t know” and neutral responses.

A lack of trust in the governments’ ability and willingness to protect their citizens’ personal data could hinder building more digitally capable bureaucracies, a goal identified by many European governments during the Covid-19 pandemic. A detailed look at the data at the national level offers a more differentiated picture (see Figure 3). Some national governments have managed to maintain citizens’ trust in their handling of personal data: Swedish (by a margin of 19 percent), German (12 percent), and British (11 percent) authorities are more trusted than distrusted by their publics when it comes to safeguarding personal data.

The fact that European citizens have less trust in their national governments than in companies from their countries to protect their personal data coincides with a broader downturn in public confidence in government institutions in Europe over the last years. Further, early research indicates that Western governments’ scrambled response to the pandemic is likely to further undermine overall public trust in government institutions.
Figure 3
European trust in safety of personal data, 2021,* percent

How confident are you in the following organizations’ ability and willingness to protect your personal data?

- Very confident / confident
- Not confident / not confident at all

<table>
<thead>
<tr>
<th>Country</th>
<th>Organization</th>
<th>France</th>
<th>Germany</th>
<th>Italy</th>
<th>Poland</th>
<th>Sweden</th>
<th>United Kingdom</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Your employer</td>
<td>34 %</td>
<td>41 %</td>
<td>38 %</td>
<td>43 %</td>
<td>40 %</td>
<td>44 %</td>
</tr>
<tr>
<td></td>
<td>Tech companies in your country</td>
<td>27 %</td>
<td>34 %</td>
<td>30 %</td>
<td>34 %</td>
<td>35 %</td>
<td>38 %</td>
</tr>
<tr>
<td></td>
<td>Your national government</td>
<td>28 %</td>
<td>38 %</td>
<td>30 %</td>
<td>26 %</td>
<td>33 %</td>
<td>27 %</td>
</tr>
<tr>
<td></td>
<td>European companies</td>
<td>18 %</td>
<td>24 %</td>
<td>27 %</td>
<td>25 %</td>
<td>21 %</td>
<td>37 %</td>
</tr>
<tr>
<td></td>
<td>Other European governments</td>
<td>16 %</td>
<td>16 %</td>
<td>22 %</td>
<td>21 %</td>
<td>19 %</td>
<td>21 %</td>
</tr>
<tr>
<td></td>
<td>US tech companies</td>
<td>12 %</td>
<td>14 %</td>
<td>22 %</td>
<td>25 %</td>
<td>15 %</td>
<td>21 %</td>
</tr>
<tr>
<td></td>
<td>US government</td>
<td>10 %</td>
<td>9 %</td>
<td>15 %</td>
<td>8 %</td>
<td>9 %</td>
<td>13 %</td>
</tr>
<tr>
<td></td>
<td>Chinese tech companies</td>
<td>7 %</td>
<td>8 %</td>
<td>14 %</td>
<td>7 %</td>
<td>12 %</td>
<td>12 %</td>
</tr>
</tbody>
</table>

*Excluding “don’t know” and neutral responses.

Data: Kekst CNC, commissioned by the Munich Security Conference. Illustration: Munich Security Conference.
A proximate cause for a low level of trust may be the perception of a distinct lack of government action felt by a large part of the public. Across all countries, our survey finds that either an absolute majority or a plurality of respondents think that their national government is not acting aggressively enough on a range of security and privacy related issues (see Figure 4).

**Figure 4**
**Public opinion on government action, 2021,* percent**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Not aggressive enough</th>
<th>Just right</th>
<th>Too aggressive</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulating how technology companies deal with data</td>
<td>45 %</td>
<td>34 %</td>
<td>4 %</td>
<td>17 %</td>
</tr>
<tr>
<td>Tackling online fraud and scams</td>
<td>58 %</td>
<td>25 %</td>
<td>4 %</td>
<td>13 %</td>
</tr>
<tr>
<td>Protecting your data</td>
<td>49 %</td>
<td>34 %</td>
<td>4 %</td>
<td>13 %</td>
</tr>
<tr>
<td>Protecting against foreign cyber threats</td>
<td>48 %</td>
<td>32 %</td>
<td>4 %</td>
<td>17 %</td>
</tr>
</tbody>
</table>

Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

**Ideas of “Techno-nationalism” as a Threat to European Action**

Moreover, our survey reveals that while there is a moderate trust deficit in some publics toward their own national governments, the lack of digital trust is much more prevalent toward the rest of Europe. Overall, respondents were significantly (by a margin of 18 percent) less trusting of private companies from elsewhere in Europe than of companies in their home country, and even less trusting of other European governments (see Figure 2). A notable exception is Poland, where respondents were especially skeptical of their own government, even more so than of others in Europe (see Figure 3). Among the rest, the gap between the perceived trustworthiness of other European governments and one’s own ranged from a margin of 11 percent in Italy to 47 percent in Sweden.
This prevailing trust gap between the national and the European level raises questions about how the efficacy of European frameworks and institutions to govern the issue of data privacy has been received by citizens. It also questions whether the EU will be able to deliver on its ambition to be a “regulatory superpower.”

The EU’s flagship measure on data privacy, the General Data Protection Regulation (GDPR), in particular, has been noted as an “export hit.” Measured against that level of ambition, the implication that the much-discussed GDPR has so far been unsuccessful in building confidence among Europeans that their data is protected equally throughout the EU should be cause for concern. The “unique selling point” of digital regulation “made in Europe” will only materialize if it also succeeds in gaining public acceptance at home.

Europeans’ concern about technology actors beyond their national borders is not limited to the handling of their personal data. The survey reveals a widespread sense among Europeans that their countries are too reliant on technologies from elsewhere, even from other European countries. What is more, our findings carry a worrying implication for how the EU is seen (see Figure 5): Overdependence on EU neighbors is seen as a problem by nearly as many Europeans as overdependence on the United States or China is.

Following this train of thought could lead to a mistaken idea of "going it
alone.” Such “techno-nationalism” that erroneously assumes EU countries could or should claim national control over digital issues would hinder efforts to deepen European integration in the digital space. Respondents to our survey are not optimistic about Europe’s chances of reversing the trend of technological overreliance on the US and China. Overall, 43 percent expected Europe to continue falling behind the United States and China over the next ten years. Another 35 percent at least believe Europe will be on par with the competition in 10 years, but just six percent expect Europe to take the lead. These numbers hint at an underlying skepticism that Europe will manage to create the fertile environment for innovation in digital tech necessary to compete. Given the digital economy’s critical importance to future growth, this should raise concerns for Europeans’ optimism about the overall prospects for European prosperity.

The results underscore the importance of long-standing priorities on the European technology agenda to enforce a positive perspective for Europe in the digital sphere: The Digital Services and Digital Markets Acts, the completion of the Digital Single Market, and the strengthening of Europe’s digital ecosystem. Europe needs to foster its market power in the digital sphere through combining member states’ weight to achieve more influence and prosperity. By achieving tangible results, the EU can counter the narrative that Europe does not deliver for its citizens when it comes to the digital economy. Otherwise, European national leaders could be confronted with
increased political pressures to attempt greater “digital independence” from the rest of the European Union, which could drive a greater wedge between member states.

**The Transatlantic Partnership: Deeply Distrusted?**

The skepticism among Europeans toward European companies and governments was compounded when our survey asked them to look across the Atlantic. The sharp decline of European confidence in the United States between 2016 and 2020 is well documented. In the digital space, however, the trend has roots that predate and go beyond the presidency of Donald Trump. The trust in the transatlantic partnership on data issues clearly has suffered continuous damage from a cascade of disputes and scandals. The 2013 Snowden leaks about the National Security Agency’s (NSA) “Prism” program, including illegal “eavesdropping” on German Chancellor Merkel’s mobile phone, was a watershed, but issues like the controversy around Cambridge Analytica’s reported leveraging of social media data and numerous widely publicized spats between US tech giants and European regulators have reinforced the trend. Moreover, it is not just that European citizens are suspicious of the US government; business relations with the United States in the tech sector are strained, too, as a recent German study finds. In some European countries today, as former Swedish Prime Minister Carl Bildt writes, US tech giants are dramatized as “mortal threats to the European way of life.”

This dramatic assessment is to some extent borne out by our polling. The US tech sector and, even more so, the US government are severely distrusted by European publics with respect to their regard for data privacy and security, even compared to the low levels of trust in domestic and other European actors (see Figure 3).

Meanwhile, a plurality of Europeans polled said they were not comfortable with US companies being involved in national critical sectors (see Figure 7). A significant share of respondents across Europe are uncomfortable with US companies being involved in social networks, mobile data, IT in healthcare, and defense and security. These concerns were heightened when extended to China. Europeans are even more uncomfortable with Chinese involvement in these sectors: Nearly half of all people surveyed are not comfortable with Chinese companies being involved in any of the areas in question. The greatest area of concern was defense and security. This underscores a trend
particularly visible in strategic decisions about technology procurement: Increasing numbers of European countries have joined the United States in practically barring Chinese suppliers from providing components to national security infrastructure and hardware (e.g., 5G equipment).\(^{40}\)

**Figure 7**  
**European discomfort with foreign companies being involved in national critical sectors, 2021,* percent**

<table>
<thead>
<tr>
<th>Sector</th>
<th>Not comfortable</th>
<th>Comfortable</th>
<th>Neutral</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Companies from the US</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT in healthcare systems</td>
<td>38 %</td>
<td>23 %</td>
<td>30 %</td>
<td>9 %</td>
</tr>
<tr>
<td>Mobile data networks</td>
<td>36 %</td>
<td>23 %</td>
<td>32 %</td>
<td>8 %</td>
</tr>
<tr>
<td>Defense and security</td>
<td>39 %</td>
<td>22 %</td>
<td>31 %</td>
<td>8 %</td>
</tr>
<tr>
<td>Social networks</td>
<td>39 %</td>
<td>22 %</td>
<td>31 %</td>
<td>8 %</td>
</tr>
<tr>
<td><strong>Companies from China</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT in healthcare systems</td>
<td>45 %</td>
<td>20 %</td>
<td>27 %</td>
<td>8 %</td>
</tr>
<tr>
<td>Mobile data networks</td>
<td>44 %</td>
<td>20 %</td>
<td>28 %</td>
<td>7 %</td>
</tr>
<tr>
<td>Defense and security</td>
<td>51 %</td>
<td>17 %</td>
<td>24 %</td>
<td>8 %</td>
</tr>
<tr>
<td>Social networks</td>
<td>48 %</td>
<td>18 %</td>
<td>27 %</td>
<td>8 %</td>
</tr>
</tbody>
</table>

Data: Kekst CNC, commissioned by the Munich Security Conference.  
Illustration: Munich Security Conference.  
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.*
Overall, our survey reveals a dire state of transatlantic digital trust in public opinion. A significant part of the European public is reluctant to rely on US actors to protect their personal data or provide technologies in key areas of the digital sector. In some countries, the US government is seen as just marginally more trustworthy than the Chinese government. Caution regarding China would appear warranted given its track record on surveillance and digital governance. By comparison, the numbers show just how much European confidence in US rule-of-law mechanisms for tech governance and data collection lags behind what should be expected vis-à-vis a democratic partner and ally. While policy-makers have again begun to invoke a basis of common values on which transatlantic cooperation on technology and even a global democratic governance for the digital world should be built, our polls show a highly skeptical European public.

Toward Security: The Mandate for Building Digital Trust

However, there is a silver lining. Our survey also reveals clear priorities among the European public, outlining the central issues European leaders need to address and signaling a mandate to take decisive action. We find that for Europeans, security is the essential element of a European, and by extension transatlantic, agenda on digital technology (see Figure 8). By a wide margin (across Europe, 38 percent of respondents name security as their first priority), the polling finds, their overriding concern is that they themselves are secure when using the internet – and they expect their governments to prioritize accordingly. Making sure tech companies “pay their fair share” of taxes garnered the next most support, while other proposed options rank much lower.

With tangible progress on consumer security issues such as protecting users from cybercrime, reducing online fraud, and ensuring security of software and hardware products, there is a high likelihood that transatlantic cooperation can be successful. The clarity of the mandate and the priority for citizens suggest a major payoff in terms of transatlantic digital trust if progress can be achieved. Reaching out to the United States on this issue will face little in the way of resistance. Other, lower-ranking priorities could be harder to achieve. Washington has been more reluctant to levy taxes on big technology firms, despite insistence from the European Commission as well as from France, in particular. A digital services tax at the European level has so far made little headway due to opposition among member states – and, prominently, from the United States – prompting France and others to go it...
Figure 8
Priorities for government action on digital technologies according to Europeans,* 2021, percent

What should be the top priority of European countries on digital technologies?

France
- User security: 30%
- Fair taxation of tech companies: 24%
- That European companies are successful: 14%
- That companies respect European values: 10%
- Low prices: 9%

Germany
- User security: 39%
- Fair taxation of tech companies: 14%
- Low prices: 12%
- That companies respect European values: 12%
- That European companies are successful: 11%

Italy
- User security: 37%
- Fair taxation of tech companies: 20%
- That European companies are successful: 15%
- Low prices: 11%
- That companies respect European values: 10%

Poland
- User security: 50%
- That European companies are successful: 15%
- Low prices: 12%
- That companies respect European values: 9%
- Fair taxation of tech companies: 9%

Sweden
- User security: 38%
- That European companies are successful: 14%
- That companies respect European values: 14%
- Fair taxation of tech companies: 11%
- Low prices: 9%

United Kingdom
- User security: 34%
- Fair taxation of tech companies: 21%
- That European companies are successful: 12%
- That companies respect European values: 9%
- Low prices: 8%

Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*Excluding “don’t know” and “none of the above”
alone. However, success on issues of user security could establish a baseline of trust that creates opportunity to achieve progress in other fields by demonstrating responsiveness to the Europeans’ most pressing concern.

A wide range of policy options in pursuit of those priorities are popular with Europeans (see Figure 9). Consistent with their concern about personal security online, respondents strongly support a mandatory cybersecurity certification for software and hardware. Recognizing that certification plays a critical role in increasing security and, perhaps more importantly, trust among technology users, the EU is working on designing a cybersecurity certification framework for assessing different products and services. While subjecting products to these schemes will remain voluntary for the foreseeable future, the private sector shows promising signs of proactively addressing the concern of cybersecurity, including initiatives such as the Charter of Trust, initiated by the MSC and companies including Siemens, Allianz, and Airbus.

In most countries, a majority also endorses requiring governments to exclusively use open-source software. A policy measure usually not exposed to much public discussion, governments’ use of open-source software is often associated with improving cost efficiency and increasing transparency and trust. Awarding government technology contracts to European companies only also received significant support across countries. Notably, a similar share of Europeans also supported banning certain foreign digital technology companies.

However, the survey data also shows that for many Europeans, concerns about preventing security risks or loopholes in personal devices ends at their own pocketbooks (see Figure 10). Despite the low levels of confidence about involving US and Chinese companies in key technology areas, only a minority of respondents indicated a willingness to pay a 30-percent premium for their technology products if it meant that they were produced only by European companies (32 percent) or in accordance with certified security standards (34 percent). These findings cannot be encouraging for proponents of European “digital sovereignty.”
Overall, our survey found a widespread lack of confidence in the entities that run and regulate the digital landscape which European citizens navigate daily. Yet, its results also indicate there is a broad basis of support for more ambitious measures that both national and European regulators can take to tackle the challenges that the digital space poses in terms of insecurity and distrust.
Please say if you would or would not be willing to pay 30 percent more for...

Figure 10
Europeans willing to pay a premium for more secure technology products, 2021, percent

- Yes  - No  - Don’t know

... a data connection using only network infrastructure produced and operated in the EU or your country

... hardware with all key components designed in EU or your country

... hardware with all key components designed with high security standards

Data: Kekst CNC, commissioned by the Munich Security Conference.
Illustration: Munich Security Conference.
*General population in France, Germany, Italy, Poland, Sweden, and the United Kingdom.

Conclusion: Reducing the Trust Deficit

Against the backdrop of digital technology’s indispensable and growing role across all sectors of society, our survey results indicating a pervasive sense of insecurity and skepticism toward actors in the digital arena are concerning. If Europe and the transatlantic partnership are to live up to their goals for integration and cooperation in the digital sphere, they will need to address this trust deficit. The implications for how the European and transatlantic partners can tackle digital distrust are two-pronged.

First, Europe needs to get its digital house in order. The EU and European governments have, so far, not convinced their publics of their collective capability to provide sensible, robust, and most of all trusted guardrails to the digitalization permeating citizens’ lives. The goal of “protecting Europeans online” – part of the broader vision of a “Europe that protects” – has not yet been achieved. Recognizing that shortcoming, EU Commission Vice-President Margrethe Vestager has said that the EU strategy for a “digital decade” has to be “as much about building trust as it is about investing in digi-
tal innovation.”49 The urgency and scale of the challenge of building trust is indeed high, but the potential rewards are also significant. On this issue, Europe needs to deliver. What is more, it needs to strengthen its foresight capabilities to identify similar challenges emerging from novel technologies early on – a goal the MSC is working toward with its recently established Security Innovation Board.50 But Europe’s performance on current challenges leads to an additional issue: Our survey finds that low confidence in Europe runs parallel to intense pressure on national governments to act. Retreating to the national level to address issues of digital technology would be counterproductive: Letting such mistaken ideas about a techno-nationalism run unchallenged would result in a “fragmented system, with different rules in different EU countries.”51 This could be especially detrimental, further weakening the EU’s ability to deliver on its promise of prosperity and thereby motivating even less investment in European cooperation.

Moving beyond rhetoric, the best way to build trust is by achieving tangible outcomes for European technology users. The priority that our respondents give to the security of their experience online gives European policymakers a clear mandate for common action toward that goal and a lens through which to view initiatives like the Digital Services and Digital Markets Acts, the completion of the single digital market, and the strengthening of Europe’s digital ecosystem. To what extent they shore up citizens’ confidence in the digital technology landscape and in Europe’s ability to effectively manage it will be a key indicator for judging the success of these initiatives. Doing so would go a long way toward backing up the popular narrative of the EU as a regulatory “trailblazer” and “superpower.”52

Second, the transatlantic partners will have to work together to manage this lack of trust and avoid letting it derail a budding transatlantic digital agenda. As such, transatlantic cooperation in this sphere will require both policy alignment across a complex set of issues, and public outreach to “win hearts and minds,” especially on the European side. The ignominious failure of the Transatlantic Trade and Investment Partnership (TTIP) is a cautionary example of the power that unfavorable public opinion wields in the potential derailment of major transatlantic initiatives. The growing drumbeat around regulating tech giants in the United States and milestones like California’s data privacy act are a hopeful sign of a real “growing convergence of views on tech governance between Europe and the United States.”53 How tech companies on both sides of the Atlantic respond will play a major role. The results of our survey can be understood as call to action to the private sector to
shore up digital trust, too. More initiatives like the Charter of Trust can go a long way toward advancing that goal.

Creating positive momentum amidst a distrust-ridden landscape requires more than gradual convergence and conciliatory rhetoric from both sides of the Atlantic. Just as there is no turning back the clock on other transatlantic issues under the new Biden administration, there is no returning to a time before the Snowden revelations, the Trump presidency, and the European digital sovereignty debate. Thus, a transatlantic tech agenda will need to include mechanisms that assure the public that they are built not just on professions of common values, but on transparency and accountability, too.

“Digital distrust” directly impacts citizens’ everyday lives. Overcoming distrust by launching a common digital agenda will be a litmus test for a transatlantic partnership that seeks to reset itself and produce tangible and effective outcomes. The pay-off would not only be a major win for transatlantic cooperation. Shaping the beginnings of a robust “digital economy rulebook” between the US and Europe – a rulebook that is trusted by their citizens – would be a step toward the goal set by the transatlantic leaders at the virtual gathering in Munich: sending a message to the world that democracies can still deliver tangible results on the major challenges of today and tomorrow.

“Together, we could create a digital economy rulebook that is valid worldwide. A set of rules based on our values: human rights and pluralism, inclusion and the protection of privacy. We need to join forces and protect these values with all our energy.”

Ursula von der Leyen, President of the European Commission, MSC Special Edition, February 19, 2021
Key Points

1. A joint tech agenda is one of the key priorities of the transatlantic partnership. Progress on this issue will serve as a litmus test for the ability of the EU-US partnership to deliver on critical issues.

2. An exclusive opinion survey commissioned by the Munich Security Conference finds that European citizens are deeply concerned about their security and that of their personal data when online. They also worry about national dependency on foreign suppliers of digital technologies.

3. Europeans have significant digital distrust in private and government institutions from other European countries, but especially the United States and China. They worry that Europe as a whole will fall further behind in the next decade.

4. European leaders need to address their citizens’ security and privacy concerns, both on the European level and within the transatlantic partnership. Otherwise, they threaten to derail transatlantic cooperation on technology and the EU’s credibility as a “regulatory superpower.” Succeeding, however, could promote meaningful progress toward common democratic technology governance.
Endnotes


12 Ulrike Franke, “Upstaged: Europe’s Struggles to Play the Great Tech Game,” London: ECFR, Commentary, February


20 Franke, “Artificial Divide.”


40 Gramer, “Trump Turning More Countries in Europe Against Huawei.”


Minister Heiko Maas on European Digital Sovereignty on the Occasion of the Opening of the Smart Country Convention of the German Association for Information Technology, Telecommunications and New Media (Bitkom),” Berlin: Bitkom, October 27, 2020, https://perma.cc/78Y4-WV9C.


**Image Sources**

MSC/Koch
P. 5

MSC/Koerner
P. 22

MSC/Niedermüller
P. 15

Unión Europea en Perú
P. 13

All other images: MSC/Kuhlmann
Acknowledgments

The Munich Security Conference would like to thank the Landesamt für Sicherheit in der Informationstechnik for supporting this project.

The authors would like to thank the entire team at Kekst CNC, as well as Marcel Lewicki and Melissa Hanlon, for their indispensable support in putting together this Munich Security Brief.
Imprint

Editorial Board
Ambassador Wolfgang Ischinger, Ambassador Boris Ruge,
Dr. Benedikt Franke, Dr. Tobias Bunde

Authors
Simon Pfeiffer, Randolf Carr

Managing Editors
Dr. Julian Voje, Laura Hartmann

Strategic Cyber Security Activities Lead
Ulrike Strauß

Layout Felix Kirner
Design MetaDesign

Stiftung Münchner Sicherheitskonferenz gGmbH
Karolinenplatz 3
80333 Munich
www.securityconference.org
research@securityconference.org

Visit our app and social media channels:
www.linktr.ee/MunSecConf

DOI: https://doi.org/10.47342/REFQ1817

Please cite as: Simon Pfeiffer and Randolf Carr, Error 404 – Trust Not Found: A European Survey on Digital (Dis)trust (Munich Security Brief 2/2021, March 2021), Munich: Munich Security Conference,
https://doi.org/10.47342/REFQ1817.

ISSN (Online): 2702-6574
ISSN (Print): 2702-6558
About the Munich Security Conference (MSC)
The Munich Security Conference is the world’s leading forum for debating international security policy. In addition to its annual flagship conference, the MSC regularly convenes high-profile events around the world. The MSC publishes the annual Munich Security Report and other formats on specific security issues.

The Munich Security Briefs
With its Munich Security Briefs, the MSC aims at contributing to ongoing debates on a particular issue within the broad field of international security. A much more concise format than the Munich Security Report, the briefs are meant to provide an overview of an issue or a read-out of a particular MSC event as well as a succinct analysis of its policy implications and strategic consequences. They generally express the opinion of their author(s) rather than any position of the Munich Security Conference.