

Mind your Privacy: American Tech Companies and Germany's Privacy Laws

Heiko Wiggers, Ph.D.

Assistant Professor of German

Wake Forest University

Department of German and Russian

Greene Hall 335, P.O. Box 7353

Winston-Salem, North Carolina 27109

United States of America

E-mail: wiggerh@wfu.edu, Phone: (336) 758-5360 (work)

Abstract

The spring and summer months of 2010 has seen several large American tech companies running into problems with Germany's privacy laws. This article is a discourse analysis that examines the companies' positions as well as the German authorities' and German public's point of view in a series of incidents that have upset relations between Germany and American tech companies. This article also discusses whether the disputes stem from a wrongful assessment of the German culture on part of the American companies and an unwillingness to adapt their products and business models to the German market. Finally, this article reflects on if and how much longer Germany can effectively enforce its stringent data protection laws in an age of ever-accelerated digitalization.

Keywords: Business studies; International relations; Business ethics; Information science; Media studies.

1.) Germany's privacy laws

Due to the horrible abuses of privacy that Germans suffered during the Third Reich (1933-1945) at the hands of the *Gestapo* ("Geheime Staatspolizei" – *Secret State Police*), and then again in the German Democratic Republic (East Germany, 1949-1990) at the hands of the *Stasi* ("Staatssicherheit" – *State Security*), the united Germany has some of the strictest data protection and privacy laws in the world. Various significant episodes in post-war Germany have been brought about by the fear of being singled out and persecuted by the government due to breaches of privacy. In May 1968, for instance, the largest protests since the end of W.W.II erupted in West Germany when the government at that time (a *Grand Coalition* of Social Democrats and Christian Democrats) passed the so-called German Emergency Acts (*Notstandsgesetze*), which would place limitations on the privacy of correspondence and the confidentiality of postal and telecommunications in cases of national emergencies. In 1970, the federal state of *Hessen* what was then West-Germany introduced the first Data Protection Act ever into its state constitution. In 1983, Germany's Supreme Court, the *Bundesverfassungsgericht* (Federal Constitutional Court), struck down an attempt to conduct a census by the then center-right government coalition of Christian Democrats and Libertarians on the grounds that several of the questions in the census form violated the private sphere of German citizens. In 1990 and again in 2009, the existing Data Protection/Privacy Laws were deemed insufficient and considerably rigidified by an overall majority in the German *Bundestag* (Parliament). The amendments made in 2009 to the Federal Law, the *Federal Data Protection Act*, are an explicit step to protect German citizens from corporate data collection practices. It prohibited, amongst other things, the processing and use of personal data for the purposes of marketing and/or selling addresses; and provided greater protection for the collection, processing, and use of employee data. It also significantly strengthened the powers of data protection authorities, who, under the new law, can fine companies for violations and in serious cases prohibit them from doing business in Germany.

The new laws were widely seen as a cautioning to corporations to consider implementing a more holistic approach with regards to their business activities, and accentuated the Germans' concern that Internet digitalization was progressing at a too rapid pace that left users' privacy vulnerable.

2.) Innovation or Violation

In March 2006, the European Union formally adopted a Data Retention Directive (Directive 2006/24/EC), which requires member states to ensure that communication providers retain, for a period of between six months and two years, data to identify the source, time, date, duration, destination, and type of a communication. This law, which was passed after the 2004 terrorist attacks in Madrid and London, was initially seen as integral to improving security and thwarting potential terrorist activities.

However, after its passage several EU member states (Austria, Germany, Ireland) questioned the legality and necessity of data retention, and in 2010, the German Federal Constitutional Court found that the Directive contravened Germany's constitution. The EU later retracted from its own directive and in general advises communication providers not to store data any longer than six months. Of specific concern for EU officials was (and is) the fact that communication providers store Internet users' IP Addresses.¹

In January 2010, the American software company Microsoft was the first non-European company to comply with the EU's recommendation and cut its data retention in their search engine *Bing* from 18 months to 6 months after which they will be removed completely. The American Internet Search company Google, however, balked at the EU guidelines and refused to reduce its data retention rate keeping the storage period of its server logs² between 18 to 24 months. As early as 2007, the Working Party, an independent EU advisory group for "the Protection of Individuals with regard to the processing of Personal Data", began to investigate Google's privacy practices. In a letter to Google, the Working Party asked whether the company had "fulfilled all the necessary requirements" to abide by EU privacy rules. The letter also specifically reminded Google that they operate under European law in Europe:

"Although Google's headquarters are based in the United States, Google is under legal obligation to comply with European laws, in particular privacy laws, as Google's services are provided to European citizens." (May 16, 2007)

The Working Party furthermore inquired as to why Google sees it necessary to store users' data at all.

"The Working Party would also be keen to hear Google's legal justification for the storage of server logs in general." (May 16, 2007)

In their answer letter – posted on its blog - Google stated that they use the same privacy protection for all countries in the world, and that creating different privacy standards for different countries would be technically impossible:

"Google provides one level of privacy protection for our users worldwide, irrespective of the country where they reside. [...] Moreover, it's extraordinarily difficult to operate a global Internet service according to different privacy standards in different countries."
(June 12, 2007)

As to abiding to European laws, the company stated:

"Google is a U.S. company and we respect U.S. laws. [...] It is important to remember that in the U.S., the Department of Justice and others have called for a 24-month data retention period. Thus, there seems to be an emerging international consensus on 24 months. [...] We therefore believe that this is a proportionate period for the retention of log data." (June 12, 2007)

The company's defiance and especially its position that U.S. policies with regards to data retention are equal to an "international consensus" infuriated European officials. Although the EU asked Google repeatedly to change its policies it refrained, however, from taking legal steps against the company since its 18-24 month retention period represented the maximum period of data retention that was allowed by the EU's own directive. Finally, in early 2010 Google agreed to "anonymize" IP addresses on its server logs after nine months. In a rather complacent statement – again posted on its own blog – the company declared:

"Although that [changing from 24 to 9 months] was good for privacy, it was a difficult decision because the routine server log data we collect has always been a critical ingredient of innovation."

The nine-month period, however, is still not in compliance with European requests. Moreover, European officials have inquired what exactly "anonymizing" data entails.³ Google again explained the purpose of data retention with "making improvements to search quality". The Working Party continues to press Google to reveal why data retention for more than six months is necessary for any purpose.

¹ An IP Address is a number which identifies the location of a web user. In theory this unique number can be used to identify the user.

² Server logs are logs that maintain a user's history of requested Internet pages and can be linked to the user's identification.

³ So far, Google has not said which actions are involved in this process.

In June 2010, while the dispute about data retention between the EU and Google was still simmering, German authorities launched an investigation of the California-based social network company Facebook for mining the accounts of its German users to gain access to and collect data about non-users. Facebook users have the option to display their e-mail contact list on their Facebook pages through an “invitation and address-book synchronization” feature. According to Johannes Caspar, the Commissioner for Data Protection and Freedom Information of the City of Hamburg (*Dienststelle für Datenschutz und Informationsfreiheit*), this resulted in Facebook using the data of “third parties” (i.e. non-users) for marketing purposes in Germany. Caspar reported that his office decided to start an investigation after they had received “many” complaints from Internet users who had received solicitations from Facebook.

The conflict in Germany came at a sensitive time for Facebook who had been accused earlier in the year (along with other social networking sites) to have sent personal and identifiable data of its U.S. users to large advertising companies. When Facebook-founder Mark Zuckerberg was pressed for comments regarding the privacy practices of his company, he told a live audience in San Francisco in early January:

“People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time. [...] Doing a privacy change for 350 million users is not the kind of thing a lot of companies would do. But we viewed that as a really important thing [...], and we decided that these would be the social norms now and we just went for it.”

(San Francisco *Crunchie* Awards, January 10, 2010)

Mr. Zuckerberg’s comments, which indirectly imply that Facebook does not merely follow new social norms but that it is setting these norms through its own practices, met with criticism from data protection advocates in the U.S. and other countries. Mr. Zuckerberg later defended his position in an op-ed piece in the *Washington Post* (May 24, 2010) but conceded that his company may have “missed the mark” with regards to privacy issues and promised Facebook users “easier control over their information”. The reactions by the European Union and Germany to Google’s and Facebook’s privacy practices should have perhaps alerted the companies to adopt a more wholesome business approach in Europe. However, Google’s next endeavor in Germany and a new Facebook feature in the United States gave cause to even greater controversy.

3.) *Street View* and Places

In the summer of 2010 Google started with the introduction of its *Street View* feature in more than twenty German cities⁴. Already a popular program in the U.S and twenty two other countries, *Street View* is a technology that provides online panoramic views of buildings from various positions. To achieve this feature, Google sends out cars and vans equipped with state-of-the-art technology that take pictures of buildings both residential and commercial. When the first Google vans started rolling through German streets, however, a storm of protests erupted. The vans were viewed by Germans as “surveillance trucks” and the feature itself was regarded as a stark attempt to compromise German privacy laws. When the company did not respond to complaints, the German government weighed in on the dispute and demanded that Google must give citizens the alternative to opt out of *Street View*. In an interview with the news magazine *Der Spiegel*, the German Minister for Consumer Protection Ilse Aigner (CSU) condemned Google’s short-term notification to the German government of its project and stated that *Street View* would violate personal rights:

“Es gibt Unterschiede zwischen einem öffentlichen Gebäude wie meinem Ministerium oder einem Wohngebiet, wo man das Kinderspielzeug im Garten erkennen oder durchs Wohnzimmerfenster fotografieren kann.“

(*Der Spiegel*, August 19, 2010)

There are differences between a public building like my office or a residential area where one can see toys in the yard or take pictures through the living room window. – my translation

The conflict with Google was aggravated when it emerged that the company inadvertently intercepted Internet data and e-mail fragments from unsecured home wireless networks while compiling its *Street View* archive in Germany. This caused Johannes Caspar’s office in Hamburg to launch a criminal investigation of Google.

⁴ The cities are: Berlin, Bielefeld, Bochum, Bonn, Bremen, Dortmund, Dresden, Duisburg, Düsseldorf, Essen, Frankfurt am Main, Hamburg, Hannover, Köln, Leipzig, Mannheim, München, Nürnberg, Stuttgart, and Wuppertal.

When German authorities demanded that the company turn over the data, Google balked and stated that Germany's own privacy laws would prevent them from doing so:

“As granting access to payload data creates legal challenges in Germany, which we need to review, we are continuing to discuss the appropriate legal and logistical process for making the data available.”

(New York Times, May 27, 2010)

Simon Davies, the director of Privacy International, a London-based organization for data protection, commented on Google's refusal:

“[The] refusal to hand over data will be seen as a declaration of war by European regulators. This is about sovereignty and a country's right to determine on its citizens' behalf what is right and what is wrong.”

(New York Times, May 27, 2010)

Of particular concern in the controversy surrounding the *Street View* project was a bill signed into law in 2004 by then Chancellor Gerhard Schröder and the German President Horst Köhler that protects citizens from “unauthorized picture recordings”.

This law (§ 201a of the German Penal Code) specifically shields German citizens from pictures that “violate the personal sphere of life” (*die den höchstpersönlichen Lebensbereich verletzen*).

When Google did not reply to calls to grant an opt-out feature (*Widerspruchsrecht*) to its *Street View* project, the tone of the debate grew increasingly testy as the company found itself attacked by a growing alliance of segments of the press, citizen watchdog groups, and the government. Ilse Aigner called *Street View* “einemillionenfache Verletzung der Privatsphäre“ (*a million-time violation of the private sphere*), and publicly warned the company:

“Google kann sich in Deutschland keinen Fehler mehr erlauben.”

(Der Spiegel, August 19, 2010)

Google cannot afford another mistake in Germany. – my translation

The *Frankfurter Allgemeine Zeitung* newspaper wrote:

“Die Stasi wäre grün vor Neid, könnte sie noch die Datensammlungen und Bewegungsprofile sehen, die manche Konzerne in ihren Computern horten. Der „Schnüffelstaat“ war gestern, heute ist Google Street View. Es ist schier unglaublich mit welcher hoheitlichem Duktus Google in die Privatsphäre eingreift.“ (August 10, 2010)

The Stasi would be green with envy if they could see the data collections and collections of movements that some corporations have stored in their computers. The “snooping state” was yesterday, today it's Google Street View. The sovereign manner in which Google interferes with the private sphere is quite unbelievable – my translation.

Under pressure, the company relented and granted citizens a four week period of time to opt out of *Street View*. This concession, however, met with new criticism as the opt-out feature was introduced on such short notice that many citizens saw it as an “ultimatum” and felt pressurized by it. Furthermore, those citizens without Internet (ca. 30% of the population) who wished their houses to be deleted from *Street View* had to go online in order to do so. It was also criticized that the announcement came at a time where many Germans were on their summer vacations and thus either did not hear about it or were unable to use the option within the granted time period. Johannes Caspar, too, questioned the timing of the grace period:

“Dies lässt durchaus Zweifel aufkommen, ob Google an einer einfachen und bürgerfreundlichen Umsetzung interessiert ist.“ (Reuters, August 9, 2010)

This causes quite some doubt whether Google is interested in a simple and citizen-friendly solution. – my translation

Peter Schaar, Federal Commissioner for Data Protection, demanded a permanent opt-out feature without Internet use:

“Widersprüche müssen auch ohne Nutzung des Internet nicht nur in einem engen Zeitfenster sondern auf Dauer möglich sein.”

(Kölner Stadt-Anzeiger, August 9, 2010)

Opt-outs must be possible without using the Internet and not only within a narrow timeframe but on a permanent basis. – my translation

Google eventually granted citizens an eight-week time period and also agreed to lower the height of their cameras from 2.5 meters to 1.8 meters. Nevertheless, the company initially refused to reveal how many calls for opt-outs it had received – an action that was criticized by Aigner as “*nichtvertrauensbildend*” (“not trust building”) in an interview with the *Hamburger Abendzeitung* newspaper. When Google eventually did release numbers it transpired that by the end of October almost 250,000 households had opted out of *Street View*.

The process of opting out created its own controversy. When German Internet users downloaded the necessary forms they were greeted by a lengthy message by Google before they could proceed to the main page. The message began as follows:

“Sie haben sich entschieden, Ihr Gebäude/Grundstück vor der Veröffentlichung von Street View in Deutschland unkenntlich zu machen. Das ist sehr schade, denn diese Funktion kann für Sie von vielfachem Nutzen sein.“

You have decided to delete your residence/property from Street View in Germany. That is a real pity, because this feature can be of great use for you. – my translation

At the bottom of the message users are directed to the actual form, which besides asking for their complete address (street name, number, zip code, and place name) also requires them to locate their residence on a map of Germany provided by Google’s own Google Earth feature. After indicating their home on Google Earth, users are asked very specific questions about their residence, such as:

“Beschreiben Sie das Dach (Flachdach, Giebeldach usw.). Beispiel: „Ein Giebeldach mit braunen Ziegeln und Dachfenstern.“

Describe the roof (flat roof, pitched roof, etc.) Example: “A pitched roof with brown tiles and skylights.” – my translation

Another question asked users for “permanent characteristics” of their residence:

Geben Sie sonstige dauerhafte Merkmale ein, die uns dabei helfen könnten, die entsprechende Abbildung zu finden. Beispiel: „Vordem Gebäude stehen zwei große Fichten.“

Describe other permanent characteristics that could help us locate the corresponding image [on Google Earth]. Example: “There are two large spruce trees in front of the building.” – my translation

Germany’s data protectors were quick to point out that Google’s process to enable an opt-out from Street View defeats the very purpose of data protection by asking users to reveal even more personal data that will be stored in a data base. By late October 2010, Google conceded that removing images (“*verpixeln*”) from *Street View* was a “complex process”, and that many households would still be visible despite having opted out. Ilse Aigner’s office criticized Google for its handling of the opt-out applications:

Bei der Eile, mit der die Flut von rund einer Viertelmillion Widersprüchen bearbeitet wurde, ist leider die Sorgfalt auf der Strecke geblieben.

(Deutsche Nachrichtenagentur, November 21, 2010)

Due to the hastiness with which approximately a quarter of a million opt-out applications were handled, accuracy unfortunately got the short end of the stick.

- my translation

By late November 2010, Google started running its *Street View* project in Germany – against the wishes of a majority of Germans. In a poll conducted by Emnid – a leading German institute for market and social research – 52% of those polled stated that they are against an introduction of *Street View* in Germany.

While Google’s clash with (parts of) the German public and government has not been resolved yet, Facebook unveiled its new *Places* feature in the United States in August 2010. *Places*, also called “location sharing” and currently only available to U.S. Facebook users with an iPhone (which provides the platform), allows users to share their location with their friends via a “Check in”- application. This feature also allows users to “tag” friends and post their location as well even if the friend does not have an iPhone. A few days after its inception, however, problems started to arise when users complained that their location had been made public without their consent.

This was largely due to the fact that *Places* is enabled by default on users' iPhones and that they have to opt-out if they do not wish to share their location. Several American Data Protection groups, among them the American Civil Liberties Union (ACLU), criticized *Places* on grounds that it violates the privacy of its users. Justin Smith, founder of the blog *Inside Facebook* tried to assuage concerns by pointing out that the feature itself was not the problem but rather users' inexperience with it:

"It's a cultural thing. People need to discover what types of things are appropriate to share about their friends. [...] I expect there will be a learning process where users discover what they're comfortable with." (CNN, August 19, 2010)

While Facebook does guarantee that no user's location will be revealed without their prior approval, Mark Rotenberg, executive director of the Electronic Privacy Information Center (EPIC, Washington D.C.), criticized Facebook's default setting:

"It is unfair to people. It's a little bit like saying, 'We're not sure if you're happy, but this is how it is.' "

(CNN, August 19, 2010)

On its internal blog, Facebook has already announced its plans to launch *Places* in other countries as well:

Places is only available in the United States right now. But we expect to make it available to more countries and on additional mobile platforms soon.

(The Facebook Blog, August 18, 2010 [blog.facebook.com])

Although *Places* is primarily a Facebook-internal affair, i.e. no non-users are involved, and no date has yet been set for a *Places* introduction in Germany (its German name will be *Orte*), it is nearly a certainty – given the company's previous trials in Germany – that these new features will elicit new investigations by the German authorities.

At the time of this writing the controversies surrounding Facebook's handling of its users' data are not resolved. Instead, it seems that new disclosures appear in the media on an almost regular basis, the latest of which are reports (Wall Street Journal, October 18, 2010) that many of Facebook's most used applications have been transmitting identifiable information to advertising companies. The Wall Street Journal reports:

The issue affects tens of millions of Facebook app users, including people who set their profiles to Facebook's strictest privacy settings. The practice breaks Facebook's rules, and renews questions about its ability to keep identifiable information about its users' activities secure. (Wall Street Journal, October 18, 2010)

Finally, also in the summer of 2010, German authorities began to investigate whether the American tech company Apple was disregarding German privacy laws with the latest version of its popular iPhone (iPhone 4). In the German user manual for its new phone Apple says it reserves the right to store and forward data of its users, particularly their geographic location, to other companies:

Apple und unsere Partner und Lizenznehmer [können] präzise Standortdaten erheben, nutzen und weitergeben, einschließlich des geografischen Standorts Ihres Apple-Computers oder Geräts in Echtzeit. (from: *German iPhone 4 Apple Manual*)

Apple and our partners and license holders can collect, use, and forward location data including the geographical location of your Apple computer or device in real time. – my translation

Similar to the Google and Facebook disputes, German politicians joined the discussion and accused Apple of a "eigenwillige Auslegung deutscher Datenschutzregeln" (*idiosyncratic interpretation of German data protection rules*). Of particular concern was the fact that users have no way to protest or opt out of this feature. The German Minister of Justice Sabine Leutheusser-Schnarrenberger stated:

"Hier sehe ich Apple in der Bringschuld, die von Steve Jobs vielbeschworene Transparenz auch tatsächlich umzusetzen. Ich erwarte, dass Apple deutschen Datenschützern Einblick in die Datenbanken gewährt."

(Spiegel online, October 18, 2010)

I think Apple has the obligation to really implement the transparency so often promised by Steve Jobs. I expect that Apple will grant German data protection officers access to its data files. – my translation

German authorities also criticized the vagueness of the term “location data” (*Standortdaten*) as Thomas Hoeren, a judge for communication and media law in the city of Münster explains:

Apple erklärt nicht klar, welche Daten sie eigentlich speichern. Der Nutzer weiß nicht, was wie lange in Verbindung mit welchen anderen Informationen gespeichert wird.“ (Spiegel online, October 18, 2010)

Apple does not clearly explain which data they actually store. The user does not know which information is stored for how long in connection with other information. – my translation

Apple replied that the company was working on a response. At the time of this writing, the issue has not been resolved yet⁵.

4.) Converging on Privacy Issues: Google opts out, Facebook becomes a celebrity

In the early months of 2011, both U.S. and European legislators realized that something had to be done to address the Internet privacy issues of their respective citizens. In a series of high-level talks in Washington and Brussels regulators from both continents started working on common privacy legislation. Although specifics of this legislation still need to be discussed in more talks (scheduled for summer and fall 2011), it seems that a common consensus has been found between the U.S. and the EU. Viviane Reding, the EU’s Justice Commissioner stated:

Until recently there was a common belief that our approaches on privacy differed so much that it would be difficult to work together; this can no longer be argued.

(March 29, 2011)

William Kennard, U.S. ambassador to the EU agrees and added:

People in Europe thought we were not as concerned as we are about updating our privacy laws.

We are in support of stronger privacy rules (March 29, 2011)

Around the same time, the American companies Mozilla (the maker of *Firefox* browser), Microsoft (*Internet Explorer* browser), and Apple (*Safari* browser) all agreed to install a “Do not track” feature in their newest browsers in order to protect Internet users’ privacy. Only Google opted out of these collective efforts. A Google spokeswoman explained:

The idea of ‘Do Not Track’ is interesting, but there doesn’t seem to be wide consensus on what ‘tracking’ really means, nor on how new proposals could be implemented in a way that respects people’s current privacy controls. We’re encouraged that [our] standards... are working on these issues (cnn, April 18)

Google also made it clear that it has no plans to add a privacy feature to its browser anytime soon. Facebook, meanwhile, has been less concerned about its users’ privacy than its new status as a “Champion for Democracy”. A large part of the U.S. Media (and the company’s own official website to no small degree) have exalted Facebook’s image in the wake of the uprisings in several Arab states, such as Tunisia and Egypt, asserting that the rebellions in these countries could not have been successful without the use of social media such as Facebook or Twitter. Conservative commentator Charles Krauthammer, for example, states:

Facebook and Twitter have surely mediated this pan-Arab (and Iranian) reach for dignity and freedom. (National Review, March 4, 2011)

Other online commentators were gushing:

Facebook is the soapbox they [the protesters] stand on, and Twitter is the Megaphone through which they speak. (Online comment, March 24, 2011)

While even a NATO review calls the “Arab Spring” a “Facebook revolution”, the idea that social networking can summon up revolutions out of the ether has also met with many critics (cf. Evgeny Morozov, *The Guardian*). Whatever Facebook’s part in the uprisings in the Arab world was and still is, its’ stylizing to a tool for democracy by the U.S. Media and by Facebook itself reveals a disturbingly condescending attitude toward the Arab states by exaggerating its contribution and downplaying the accomplishments of the Egyptian and Tunisian citizens.

⁵German authorities suspect that Apple treated the Germans’ concern as negligible because Steve Jobs’ priority at the time was negotiating the Beatles song catalog for the popular iTunes program.

It is interesting to note that at the same time another North American tech company, Canada’s RIM (Research in Motion), manufacturer of the popular BlackBerry phones, was facing a ban on its phones in India on grounds that the data transmission on its devices was deemed too secretive by the Indian government and would enable militants to avoid detection.

Any concerns for privacy on Facebook have almost completely vanished over the debate (celebration?) of its role in the Arab Spring.

5.) Analysis

The privacy abuses of its past cut deep into the collective German psyche with its repercussions far from being over. A stark reminder of the past is the so-called *Gauck-Behörde*, a federal government agency that investigates the crimes of the *Stasi*.⁶ Founded in 1990 shortly after the reunification, its main purpose is the opening of *Stasi* records to the general public. At its zenith, the *Stasi* had records on some six million people including an archive of sweat and body odor samples. Every German citizen has the right to inquire at this agency whether the *Stasi* has kept a record on him or her and to gain access to their files. At the end of 2009, more than 1.8 million citizens had asked for access, with 103,000 alone for the year of 2009. The inspection of their records often produces devastating discoveries for those affected, e.g. husband spying on wife, doctors on patients, the Post Office on its customers, professors on students, neighbors on neighbors, etc. In order to avoid the excesses of the past it is therefore not surprising that Germany has instituted some of the strictest privacy laws in the world. To an outsider, however, Germany's handling of privacy issues can seem somewhat paradoxical. The following practices, for instance, are commonplace:

- It is customary to include age, marital status, number of children, and a recent passport photo in job applications. Until a few years ago, it was also required to include one's religious affiliation. Employers will not consider applications without these data.
- Germany has compulsory resident registration, i.e. every citizen must register his or her current address with the *Einwohnermeldeamt* (Residents' Registration Office). Even a change of residence in the same city requires a new entry at this office. Public access to the office is limited.
- As of 2010, many German airports have been employing full-body scanners.
- It is customary, though not a law, to have one's name printed next to the doorbell for both family houses and apartment buildings.
- German police are authorized to conduct random ID checks at public places such as train stations, soccer stadiums, or on the *Autobahn*. Having no ID or an invalid one carries stiff fines.

These procedures are considered normal by most Germans or at worst annoying, while most of them would be regarded as intrusive or even illegal in the United States.

With regards to online habits, many Germans enjoy similar activities to Americans such as posting pictures of themselves (and others) online or writing public blogs although paying for online purchases with credit card is relatively rare. It is interesting to note in this respect that Google Earth, a Google program that shows aerial photography and images (among them buildings) obtained from satellite pictures, enjoys enormous popularity in Germany.

Given the above mentioned practices one could ask the question why a majority of the German population became so upset with Google's *Street View* program. A possible answer might be that the program itself is not the point of contention but rather the manner in which Google introduced it. Indeed, one of Ilse Aigner's principal points of complaint was that Google "blindsided" the German public with its intentions:

Die Ankündigung von Google, Street View noch in diesem Jahr zu starten, ist mitten in die Sommerferien mehrerer Bundesländer geplatzt. Google hat damit vor allem viele Bürgerinnen und Bürger überrumpelt.
(Hamburger Abendblatt, August 17, 2010)

Google's announcement to start Street View already this year came in the middle of the summer vacation of several federal states. With this Google first and foremost blindsided many citizens.–
my translation

A very significant issue in this regard is the fact that citizens had to ask the company to be excluded from its project rather than the company asking citizens whether it may include them. In a German online forum about *Street View* one commentator pointed out:

⁶ The official name of this agency is *Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik* (Federal commissioner for the archives of the State Security Service of the former German Democratic Republic). It is commonly called *Gauck-Behörde* after the name of the first federal commissioner Joachim Gauck.

Zuerst einmal muß man um Erlaubnis fragen wenn man etwas haben will was anderen gehört - nicht umgekehrt.

(Online comment, August 14, 2010)

First of all you have to ask for permission if you want something that belongs to others – not the other way around. – my translation

This issue seems particularly striking considering that the German *Street View* project will in all likelihood constitute a considerable source of revenue for Google.

Although many Germans expressed anger by the sight of Google vans equipped with cameras on long tripods that parked directly in front of their houses, it should be noted that many others welcomed *Street View*. German police, for instance, stated that the program would help with traffic and with crime prevention while others expressed their sheer joy at the possibility of “armchair traveling”. “Gerda”, another online commentator, for example, remarked:

Ich freue mich schon riesig auf die Straßenansichten in Deutschland. Da ich es mir nicht leisten kann die Welt zu bereisen, so kann ich sie mir wenigstens damit auf dem Rechner ansehen.

(Online comment, August 14, 2010)

I am really looking forward to the street views of Germany. Since I can't afford to travel the world I can now at least look at it on my computer. – my translation

Yet other commentators pointed out that the pictures on *Street View* are inconsequential compared to the data collections that many governments have built up on their citizens, particularly in the wake of the 09/11 terrorist attacks.

A much more critical point than potential privacy invasion is the question whether an American company has the right to carry out its schemes in a foreign country if the majority of that country's population is against it. The manner of launching its product in Germany and proceeding with it suggests that the company not only miscalculated the German market but also misread the German mentality. In fact, during the course of the debate the German *Bundestag* discussed two pieces of legislature that might have given Google pause for thought. On August 25, an absolute majority in the Parliament banned – without exception (*ohne Ausnahme*) - video surveillance cameras at workplaces. Violations of this new law can cost employers fines between 50,000 and 300,000 Euros. A few days earlier, German Secretary of the Interior Thomas de Maiziere rejected a motion to make public the names and whereabouts of sex offenders. Both practices are commonplace and quite undisputed in the United States and highlight yet again the different notions of privacy in both countries. The concerns about *Street View* were shared by other European countries, and in March 2011 France's Data Privacy Regulator CNIL (Commission Nationale de l'information et des Libertés) fined Google for a record 100,000 Euros (\$142,000) over private information the search engine giant collected during its *Street View* panoramic project.

If Google misjudged the conditions in Germany, then many Germans seem to have a misconception of Google as well, particularly since many people still associate large American corporations with evil plots. The Germans' fear of a Big-Brother-type, all pervasive company is likely exacerbated by Google's non-physical presence in Germany. While Google's headquarters in California are generally praised for its environmental sustainability, relaxed work atmosphere, and its fair treatment and generous compensation of its workers, it might be easy for Germans to imagine a malicious behemoth that is commanded from a distance. The tone and objectivity of the debate was also not helped by somewhat exaggerated and sensationalized articles in several of Germany's largest newspapers such as “*Google weiß wo du bist*” (“Google knows where you are” – *Die Zeit* newspaper, February 2010), or “*Street View statt Schnüffelstaat*” (“Street view instead of a snooping state”, *Frankfurter Allgemeine* newspaper, August 2010).

Google's data retention practices pose legal-philosophical questions that seem quite difficult to resolve. Although it would behoove Google to respect the laws of other countries, governments have relatively few legal tools available to curb or regulate such a truly border-transcending item as an Internet search engine other than shutting it down. A different aspect in this regard is the question whether governments are entitled to such actions as long as no person is harmed. The case of *Street View* in Germany has shown that even if a government has strict privacy laws in place they can be rendered ineffective in the face of growing worldwide digitalization. Mark Zuckerberg's comments regarding privacy might be considered arrogant by some.

However, internet users become Facebook members with the intention to share things from their personal lives. As the founder and CEO of his social network it is Mr. Zuckerberg's prerogative to set its parameters as long as he does not violate any privacy laws. German politicians and privacy advocates have repeatedly pointed out that people who join Facebook – which now boasts more than half a billion members worldwide – should do so “at their own risk”, i.e. they must be prepared to meet possible privacy issues. However, the sheer number of members, including in Germany, demonstrates that online privacy does not seem an essential issue for them. Surveys in both Germany and the U.S. indicate that the younger generations (under 30) are in general much less concerned about their online privacy. Indeed, Mr. Zuckerberg's statement that people are more “comfortable [with] sharing more information” might not be an exaggeration but can rather be attributed to a fundamental change in which people communicate. The relative novelty, growing popularity, and rapidly changing features of online social networks likely also arouse suspicion of privacy advocates because they challenge the conventional notions of privacy. Although many of the more ardent members might disagree, it remains to be seen whether social networks are a fad or whether they will truly assert themselves as a medium for information exchange, communication, commerce, and science. If so, then having a Facebook account might soon be considered as mundane and normal as having an Email account or having one's name listed in a telephone directory.

6.) Conclusion

Germany's privacy laws are, obviously, a reaction to their past and are in place to avoid a repetition of the past's excesses. In conclusion, the most perplexing aspect in this matter is perhaps not the Germans' reaction but rather the Americans' insensitivity, particularly since American tech companies are usually noted for their sophistication and their attentive market research. Most vexing for the German consumers is the fact that their protests were largely ignored and that concessions were only made after German government agencies intervened on their behalf. This kind of approach did not only hurt the companies' image in Germany but it awoke old fears that Americans force their business (and politics) model upon others.

On the other hand, the German will have to ask themselves how much longer they will be able to maintain their privacy laws in the face of ever-growing digitalization. As one of the world's leading export nations, the Germans can scarcely afford in the long run privacy laws that are – however well intended – largely out of sync with those of their main trading partners. The Germans' dilemma is exacerbated if one considers that digitalization will likely become even more personal in the future, for example having medical records online. To a certain degree, Germany's privacy laws also run the risk of being counterproductive within Europe. The free flow of goods and information – one of the most significant achievements of the EU and very much advanced by the Germans themselves – could be severely compromised if the continent's economic powerhouse operates on a separate level in terms of digitalization.

Gratwanderung is a German expression that defies translation. It typically refers to a situation in which two opposing aspects need to be balanced in order to find a solution. Eventually, the Germans might have to embark on difficult, maybe even painful digital *Gratwanderung* that safeguards their values but also ensures progress and continuing global competitiveness.

References

Dou, Eva, (2011), Europe and the US are converging on the subject of Internet privacy. [Online] Available: [ITpro](http://www.itpro.co.uk/632305/european-and-us-regulators-unite-over-web-privacy), March 29, 2011. <http://www.itpro.co.uk/632305/european-and-us-regulators-unite-over-web-privacy>. Retrieved on May 15, 2011

Fischer, Sebastian; Gathmann, Florian; Nelles Roland, (2010) Google kann sich keinen Fehler mehr erlauben. [Online] Available: [Der Spiegel online](http://www.spiegel.de/politik/deutschland/0,1518,712514,00.html) 19 August 2010. <http://www.spiegel.de/politik/deutschland/0,1518,712514,00.html>. Retrieved on May 15, 2011.

Goldberg, Stephanie, (2010), New Facebook feature raises more privacy concern. [Online] Available: [cnn.com](http://articles.cnn.com/2010-08-19/tech/facebook.places.privacy_1_privacy-controls-privacy-concerns-feature?_s=PM:TECH) 19 August 2010. http://articles.cnn.com/2010-08-19/tech/facebook.places.privacy_1_privacy-controls-privacy-concerns-feature?_s=PM:TECH. Retrieved on May 15, 2011.

Ian, Paul, (2009), Does Google know too much about you? [Online] Available: [PCWorld](http://www.pcworld.com/article/168224/does_google_know_too_much_about_you.html) 10 July 2009. http://www.pcworld.com/article/168224/does_google_know_too_much_about_you.html. Retrieved on May 15, 2011.

Iken, Matthias; Kammholz, Karsten, (2010), Ministerin Aigner: Google hat viele Bürger überrumpelt. [Online] Available: Hamburger Abendblatt 17 August 2010. <http://www.abendblatt.de/politik/deutschland/article1601494/Ministerin-Aigner-Google-hat-viele-Buerger-ueberrumpelt.html>. Retrieved on May 15, 2011.

Johnson, Bobby, (2010) Privacy no longer a social norm, says Facebook founder. [Online] Available: The Guardian 11 January 2010. <http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy>. Retrieved on May, 15, 2011.

Kohler, Berthold, (2010), Street View statt Schüffelstaat. [Online] Available: Frankfurter Allgemeine Zeitung 10 August 2010. <http://www.faz.net/s/homepage/archive/.html>. Retrieved on May 15, 2011.

Krauthammer, Charles, (2011), From Baghdad to Benghazi. [Online] Available: The National Review 4 March 2011. <http://www.nationalreview.com/articles/261278/baghdad-benghazi-charles-krauthammer>. Retrieved on May 24, 2011.

Landers, Uwe, (2010), Kritik am iPhone Hersteller: Leutheuser-Schnarrenberger attackiert Apples Datensammelei. [Online] Available: Der Spiegel online 26 June 2010. <http://www.spiegel.de/netzwelt/web/0,1518,702994,00.html>. Retrieved on May 15, 2011.

Marsburg, Karin, (2010), Kritik an Google Frist. [Online] Available: Kölner Stadtanzeiger. 9 August 2010. <http://www.koelnerstadtanzeiger/archive/2010/09/Bericht.html>. Retrieved on May 15, 2011.

Morozov, Evgeny, (2011), Facebook and Twitter are just places revolutionaries go. [Online] Available: The Guardian, 7 March, 2011. <http://www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians>. Retrieved on May 15, 2011.

O'Brien, Kevin J., (2010) Google Balks at Turning Over Private Internet Data to Regulators. [Online] Available: The New York Times 27 May 2010. <http://www.nytimes.com/2010/05/28/technology/28google.html>. Retrieved on May 15, 2011.

Orlow, Dietrich. A History of Modern Germany, 1871 to Present. (fourth edition). New Jersey: Prentice Hall, 1999.

Rebermann, Erwin, (2010), Aigner kritisiert mangelnde Sorgfalt bei Street View. [Online] Available: Taz 21 November 2010. <http://www.tz-online.de/nachrichten/internet/aigner-kritisiert-mangelnde-sorgfalt-beistreet-view-1015806.html>. Retrieved on May 15, 2011.

Single, Ryan, (2011), Google holds out against „Do not track“. [Online] Available: cnn.com 18 April 2011. <http://www.cnn.com/2011/TECH/web/04/18/google.chrome.wired/index.html>. Retrieved on May 24, 2011.

Steel, Emily; Fowler, A. Geoffrey, (2010), Facebook in Privacy Breach. [Online] Available: The Wall Street Journal 18 October 2010. <http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html>. Retrieved on May 15, 2011.

OTHER WEBSITES

Apple's German iPhone 4 manual. Available at: manuals.info.apple.com/.../iPhone_3G_Wichtige_Produktinformationen_D.pdf. Retrieved on May 15, 2011.

Facebook Announcement to introduce Places to more countries. Available at: <http://www.facebook.com/blog.php?post=418175202130>. Retrieved on May 15, 2011.

Google's Opt-out application from Street View. Available at: <https://streetview-deutschland.appspot.com/submission>. Retrieved on May 15, 2011.

Google's Response to Working Party. Available at: blogs.taz.de/ctrl/files/2008/09/google.pdf. Retrieved on May 15, 2011.

NATO Review. Arab spring = Facebook revolution. Available at: http://www.nato.int/docu/review/2011/Social_Medias/Arab_Spring/EN/index.htm. Retrieved on May 15, 2011.

Working Party's letter to Google. Available at: http://www.democraticmedia.org/news_room/letters/art29togoogle. Retrieved on May 15, 2011.