

## GERMANY

In post-war Germany surveillance has always been a popular topic of discussion and study. With the legacy of two totalitarian dictatorships, first the Nazi regime from 1933–1945 and then the communist surveillance state in the East of the country (German Democratic Republic, GDR, 1945–1989/90), the topic continues to be a sensitive one. Consequently, the revelations made by Edward Snowden in 2013 about the far-reaching international Internet surveillance practices by the U.S. National Security Agency (NSA) and its British counterpart did not sit well with the German public. Practices for crime or terror prevention common in many other Western states like closed-circuit television (CCTV) surveillance of public places are widely regarded as suspicious and comparatively sparsely used in Germany. In general, there remains a good deal of scepticism against the increasing use of surveillance technology among large parts of the German public, even against usually benign practices like population censuses (especially the one in 1983), using store cards or credit cards, and ordering online. This entry reviews the basic principles of individual rights and freedoms historically granted to German citizens during different time periods, and concludes with a section about how new revelations of surveillance and threats of terrorism have altered people's attitudes.

The experience of the Nazi regime lay at the basis of the far-reaching guarantees for the private sphere in the *Grundgesetz* or “Basic Law” of the Federal Republic of Germany (1949), including the inviolability of residences (Article 13) as well as the sanctity of mail and telephone communication (Article 10). These far-reaching guarantees were tested for the first time when in the 1970s and early 1980s the West-German state was challenged by domestic left-wing terrorist groups, especially the Red Army Faction (RAF), also known by

the name of its founders Baader and Meinhof. The *Verfassungsschutz* (Federal Office for the Protection of the Constitution) and the police gained significant additional powers (e.g. *Rasterfahndung*, “dragnet investigation”) that were highly contentious at the time and pushed the boundaries of what was legally possible, but, with a few notable exceptions (e.g., the wiretapping affair around the nuclear physicist Klaus Traube in 1974) by and large still continued to comply with the letters and spirit of the post-war constitution.

Since the end of the Cold War it was particularly the legacy of the infamous and formerly omnipresent East-German Ministry for State Security (*Ministerium für Staatssicherheit*, MfS), better known by its acronym *Stasi*, that shaped the debate about surveillance in modern day re-united Germany. After all, when communism was toppled in 1989, the main ire of the revolutionary masses was directed at the Stasi spies. The organization’s headquarters in Berlin and Leipzig were stormed to shed light on the Stasi’s roughly 100,000 full-time employees and 170,000 informants or “informal collaborators” (*Informeller Mitarbeiter* [IM]), in a population of 17 million. Treatment of the personal surveillance files on millions of citizens that survived the attempt at destruction by the falling regime remained contentious for a long time. Today the files are looked after by a special government institution, guaranteeing every citizen access to their file, and periodically causing debates when politicians’ or other public figures’ real or alleged past as an IM comes to light.

Accordingly, any attempt to widen surveillance for the purposes of crime and terror prevention meets high levels of skepticism and opposition, which has led to the resignations of ministers and the end of coalition governments. When in 1998 the *Bundestag* (German parliament) reformed the legislation (Article 13 GG), enabling the acoustic surveillance of residences for the purposes of crime persecution, the law became known as *Grosser Lauschangriff* (literally translated “large wiretap attack” on private residences), as opposed to

*Kleiner Lauschangriff* (“small wiretap operation” in public areas) and had to be reformed after large parts of the act were declared unconstitutional in 2004 by the German Supreme Court (*Bundesverfassungsgericht*). Finally a reformed surveillance act that imposes very strict limitations and excludes, for example, journalists and lawyers from being targeted passed parliament in 2005, without entirely silencing its critics.

In a similar vein *Vorratsdatenspeicherung*, the retention of telecommunication data like call detail records and Internet traffic and transaction data for six months that has been introduced on the European Union level and been translated into German legislation in 2008, was declared unconstitutional in 2010. Data protection remains important in Germany and has the status of an elementary right (*Grundrecht auf informationelle Selbstbestimmung*, “elementary right on informational self-determination”), confirmed by the Supreme Court even though it is not explicitly mentioned in the constitution.

In contrast, the *Meldepflicht* (resident registration)—the obligation of citizens to register their address with the municipality (as in many other continental-European countries) or risk being fined, and the subsequent issuance of identity cards—goes largely unchallenged. This is in stark contrast to countries like the United States or the United Kingdom that do not have a similar obligation. In the case of the United Kingdom, the attempt to introduce identification cards by the former Labour government in 2008 led to major controversy. This discrepancy has been attributed to different conceptualizations of the “right to privacy” in the German and Anglophone legal traditions. Whereas the American legal tradition focuses on the “right to solitude” or being left alone by the government, freedoms that are described in part in the Fourth Amendment to the U.S. Constitution, the German concept of “informational self-determination” echoes the definition of privacy as an individual’s right to decide what personal information is communicated to others and the circumstances under which such information is shared.

The experience of terrorist attacks against the United States on September 11, 2001 and the subsequent War on Terror also led to new debates and the questioning of previous practices in Germany. After all, the atrocities of 9/11 in the United States were planned and carried out by a cell of Jihadist terrorists based in the northern port city of Hamburg, Germany. On the other hand, Edward Snowden's revelations, published by the *New York Times*, the British *Guardian*, and the German current affairs magazine *Der Spiegel* since 2013, reinforced old suspicions that were, to an extent, also shared by German officialdom. The revelation that German chancellor Angela Merkel, who grew up under surveillance of the Stasi in the GDR, was targeted by the NSA ("Stasi 2.0"), caused tensions in German-American relations, which were haphazardly repaired by U.S. President Barack Obama's public apology. Merkel's government also agreed to do its part by refraining from giving in to widespread demands to offer exile to Snowden in Germany, although other German politicians visited and negotiated with him in Moscow, Russia.

Ulrich Tiedau

*See also* Closed-Circuit Television; Cold War; National Security Agency Leaks; Right to Privacy

#### **FURTHER READINGS**

Flaherty, David H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (UNC Press Books, 2014).

Ross, Jacqueline E., 'The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany', *The American Journal of Comparative Law*, 55 (2007), 493–579.