United Kingdom

C Violations of User Rights

The government has placed significant emphasis on stopping the dissemination of terrorist content and hate speech online, and on protecting individuals from targeted harassment on social media. While users are generally free from arrest, prosecution, or extralegal violence in response to their online activity, user rights are undermined by extensive surveillance for law enforcement and foreign intelligence purposes. Several individuals were arrested in relation to online posts deemed to be hate speech, though the volume of such arrests appears to be declining. The government obtained anonymized location data from telecommunications providers to monitor trends in compliance with COVID-19 social distancing guidelines.

C1 1.00-6.00 pts0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	5.005 6.006

The UK does not have a written constitution or similarly comprehensive legislation that defines the scope of governmental power and its relation to individual rights. Instead, constitutional powers and individual rights are addressed in various statutes, common law, and conventions. The provisions of the European Convention on Human Rights were adopted into law via the Human Rights Act 1998. In 2014, Conservative Party officials announced their intention to repeal the Human Rights Act in favor of a UK Bill of Rights in order to give British courts more control over the application of human rights principles.[118] During the 2017 election campaign, Prime Minister Theresa May initially scaled back those ambitions.[119] However, in June 2017 she reopened the possibility of significantly amending human rights legislation to allow more aggressive measures against terrorism in light of high-profile attacks in Manchester and London.[120] No such legal changes were enacted during the coverage period, and as of July 2020, this point seems to have disappeared from the government's legislative agenda.

C2 1.00-4.00 pts0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	2.002 4.004

Political expression and other forms of online speech or activity are generally protected, but there are legal restrictions on hate speech, online harassment, and copyright infringement, and some measures—including a 2019

counterterrorism law—could be applied in ways that violate international human rights standards.

The Counter-Terrorism and Border Security Act, which received royal assent in February 2019, included several provisions related to online activity (see C5).[121] The legislation, intended to update the Terrorism Act 2000, came in response to attacks in London and Manchester in 2017, among other events.[122] The new provisions make it an offense to view terrorist material (as defined in the act) over the internet. Individuals can face up to 15 years in prison for viewing or accessing material that is useful or likely to be useful in preparing or committing a terrorist act, even if there is no demonstrated intent to commit such acts. The law includes exceptions for journalists or academic researchers who access such materials in the course of their work, but it does not address other possible circumstances in which access might be legitimate.[123] "Reckless" expressions of support for banned organizations are also criminalized under the law. A number of civil society organizations argued that the legislation was dangerously broad, with unclear definitions that could be abused.[124]

Stringent bans on hate speech are encapsulated in a number of laws (see Table 1), and some rights groups have said they are too vaguely worded. Defining what constitutes an offense has been made more difficult by the development of new communications platforms.

Table 1: List of Legislation Regarding Offensive Speech

Statute	Details	Maximum penalty
Public Order Act 1986	Section 5 penalizes "threatening, abusive or insulting words or behavior." In 2013, it was amended to remove insults. [125]	Unlimited fine and six months in prison
Malicious Communications Act 1988	Section 1 criminalizes targeting individuals with abusive and offensive content online "with the purpose of causing distress or anxiety." [126] In 2015, it was amended to include "revenge porn," the sharing of sexual images without the subject's consent and with the intent to cause harm. [127]	Two years in prison
Communications Act 2003	Section 127 punishes "grossly offensive" communications sent through the internet. [128]	Unlimited fine and six months in prison
Terrorism Act 2006	Section 1 prohibits the publishing of statements likely to encourage the commission, preparation, or instigation of terrorism.	On indictment, imprisonment for seven years and unlimited fine On summary conviction, imprisonment for one year and unlimited fine

The Crown Prosecution Service (CPS) publishes specific guidelines for the prosecution of crimes "committed by the sending of a communication via social media."[129] Updates in 2014 placed digital harassment offenses committed with the intent to coerce the victims into sexual activity under the Sexual Offences Act 2003, which carries a maximum of 14 years in prison.[130] Revised guidelines issued in March 2016 identified four categories of communications that are subject to possible prosecution: credible threats; abusive communications targeting specific individuals; breaches of court orders; and grossly offensive, false, obscene, or indecent communications.[131] They also advised prosecutors to consider the age and maturity of the user in question. Some observers said this could restrict the creation of pseudonymous accounts, though only in conjunction with activity that is considered abusive.[132] In October 2016, the CPS updated its guidelines again to cover more abusive online behaviors, including organized harassment campaigns or "mobbing," and doxing, the deliberate and unauthorized publication of personal information online to facilitate harassment.[133]

The Copyright, Designs, and Patents Act 1988 carries a maximum two-year prison sentence for offenses committed online. In 2015, the government held a public consultation regarding a proposal to increase the sentence to 10 years. Of the 1,011 responses, only 21 supported the proposal,[134] but a 2016 government consultation paper nevertheless announced plans to introduce an amendment that included the 10-year maximum sentence "at the earliest available legislative opportunity."[135] The penalty was ultimately incorporated into the Digital Economy Act 2017.

The libel laws in England and Wales have historically tended to favor the plaintiff, leading foreign litigants to file suits there that had only a tenuous connection to the UK, a phenomenon known as "libel tourism." The Defamation Act 2013 was intended to address the problem by requiring claimants to prove that England and Wales are the most appropriate forum for the action; setting a serious-harm threshold for claims; and codifying certain defenses such as truth and honest opinion. Defamation cases filed in London, most of which involve social media posts, increased significantly in 2019,[136] reversing a previous trend.[137]

C3 1.00-6.00 pts0-6 pts

Are individuals penalized for online activities?	5.005 6.006

Police have arrested internet users for promoting terrorism, issuing threats, or engaging in racist abuse, and in some past cases the authorities have been accused of overreaching in their enforcement efforts. The frequency of these cases appear to be declining, and prison sentences for political, social, and cultural speech remain rare.

Guidelines clarifying the scope of offenses involving digital communications may be helping to cut down on the more problematic speech-related prosecutions observed in the past (see C2). The scale of arrests remains a concern, though many investigations are dropped before prosecution. Figures obtained by the *Times* newspaper showed that in 2016 and 2017, more than 3,000 individuals were detained and questioned for offensive online comments under Section 127 of the Communications Act, 2003.[138] In Scotland, almost 8,600 people were charged under Section 127 from 2008 to 2018.[139] The devolved Scottish government is also debating changes to its legislation to address 'hate crime',[140] a bill that opposition parties believe will have a stifling effect on free speech.[141]

Local police departments have the discretion to pursue criminal complaints that would be treated as civil cases in many democracies. There is an online portal to facilitate the reporting of hate crimes to the police.142 In May 2020, police in Newcastle arrested three teenagers who posted a Snapchat video mocking the death of George Floyd, who was killed by police officers in the US earlier that month. The incident was reportedly being investigated as a hate crime;143 no updates were reported as of the end of the coverage period.

In February 2020, the High Court ruled that police officers acted unlawfully when they interviewed Henry Miller, a former police officer in Lincolnshire, in relation to tweets by Miller that mocked transgender people. The officers interviewed Miller at his workplace and informed him that the tweets would be recorded as a non-crime hate incident under the 2014 Hate Crime Operational Guidance, which encourages law enforcement to collect data on incidents motivated by prejudice that do not constitute hate crimes.144 The High Court found that the interview of Miller at his place of work curtailed his freedom of speech. The court did not invalidate the guidance, a part of the ruling that Miller plans to appeal.145

Cases of offensive humor have been prosecuted. In early 2016, for example, police in Scotland detained 28-year-old Markus Meechan after he uploaded a YouTube video of himself teaching his girlfriend's dog to perform a Nazi salute as a prank.146 Meechan was convicted of breaching Section 127 of the Communications Act 2003,147 and in April 2018 he was ordered to pay a fine of £800 ($1,000).148 In January 2019, the High Court of the Judiciary in Scotland rejected an appeal in the case.149

In another case of offensive humor from November 2018, a group of friends at a party burned an effigy of the Grenfell Tower—a public housing facility in London where a fast-moving fire had killed more than 70 people in June 2017—and posted video of the act to their WhatsApp group. The video was subsequently uploaded to YouTube, where it spread widely and received public condemnation. There was a police investigation,150 and one of the accused, Paul Bussetti, was charged under the Communications Act 2003.151 In August 2019, Bussetti was found not guilty.152

C4 1.00-4.00 pts0-4 pts

Does the government place restrictions on anonymous communication or encryption?	2.002 4.004

Users are not required to register to obtain a SIM card, allowing for the anonymous use of mobile devices.153 However, some laws provide authorities with the means to undermine encryption, and security officials have pushed for further powers.

There are several laws that could allow authorities to compel decryption or require a user to disclose passwords, including the Regulation of Investigatory Powers Act 2000 (RIPA), the Terrorism Act 2000, and the Investigatory Powers Act 2016 (see C5 and C6).154 Although such powers are seldom invoked in practice, some users have faced detention for failure to provide passwords.155

In October 2019, Home Secretary Priti Patel and her counterparts in the United States and Australia wrote to

Facebook opposing the company's plans to implement end-to-end encryption across its messaging platforms.156 The letter followed communiques in July and October 2019 from the Five Country Ministerial, of which the UK is a member, criticizing technology companies that provide encrypted products that preserve anonymity and preclude law enforcement access to content.157

In late 2018, GCHQ representatives released a proposal, the so-called "Ghost Proposal," calling for more cooperation mechanisms between communications services and intelligence bodies that would allow the decryption of criminal and terrorist communications in "exceptional" circumstances.158 The proposal would require companies to facilitate the addition of "ghost" users—law enforcement agents—to encrypted conversations without the knowledge of participants. Civil society organizations, service providers, technology platforms, and other experts criticized the idea as a serious infringement on privacy that would undermine cybersecurity.159 As of June 2020, no further developments on the proposal seem to have occurred.

A new law in 2017 requiring age verification for access to online pornography also threatened anonymity, though the government has abandoned implementation of the law because of technical limitations (see B1).

C5 1.00-6.00 pts0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	2.002 6.006

The UK authorities are known to engage in surveillance of digital communications, including mass surveillance, for intelligence, law enforcement, and counterterrorism purposes. A 2016 law introduced some oversight mechanisms to prevent abuses, but it also authorized bulk collection of communications data and other problematic practices. A 2019 counterterrorism law empowered border officials to search travelers' devices, undermining the privacy of their online activity.

The Counter-Terrorism and Border Security Act (see C2) gives border agents the ability to search electronic devices at border crossings and ports of entry with the aim of detecting "hostile activity"—a broad category including actions that threaten national security, threaten the economic well-being of the country in a way that touches on security, or are serious crimes. However, border agents do not need to have a "reasonable suspicion" that an individual is engaged in such "hostile activity" in order to initiate a search, giving them broad discretion to stop and search travelers.160 Those stopped are required to provide information when requested by border officers, including the passwords to unlock devices.161

In September 2018, the European Court of Human Rights found that parts of the UK's bulk surveillance regime under the RIPA violated the European Convention on Human Rights, specifically the law's provisions on privacy and free expression. The court noted that, for example, there were insufficient safeguards to protect confidential journalistic material.162 However, the court controversially ruled that bulk surveillance was not always incompatible with human rights and could fall within a state's "margin of appreciation in choosing how best to achieve" national security..163 The ruling addressed three petitions filed by UK civil society groups and individuals following former US National

Security Agency contractor Edward Snowden's 2013 revelations about UK surveillance.[164] Some of the problems that were raised in the case were addressed in the Investigatory Powers Act 2016 (IP Act).

The IP Act codified law enforcement and intelligence agencies' surveillance powers in a single omnibus law, whereas they were previously scattered across multiple statutes and authorities.[165] It covers interception, equipment interference, and data retention, among other topics.[166] In general, the IP Act has been criticized by industry associations, civil rights groups, and the wider public, particularly regarding the range of powers it authorizes and its legalization of bulk data collection.[167]

The act specifically enables the bulk interception and acquisition of communications data sent or received by individuals outside the UK, as well as bulk equipment interference involving "overseas-related" communications and information. When both the sender and receiver of a communication are in the UK, targeted warrants are required, though several individuals, groups, or organizations may be covered under a single warrant in connection with a single investigation. Moreover, the internet's distributed architecture means that privacy protections based on an individual's physical location are highly porous. Communications exchanged within the UK may be routed overseas, a fact that intelligence agencies have exploited in the past to conduct bulk surveillance programs like Tempora (see below).

Part 7 of the IP Act introduced warrant requirements for intelligence agencies to retain or examine "personal data relating to a number of individuals" where "the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions."[168] Datasets may be "acquired using investigatory powers, from other public sector bodies or commercially from the private sector."[169] Under Section 220, an initial examination of bulk datasets must occur within three months "where the set of information was created in the United Kingdom" and within six months otherwise.

The IP Act established a new commissioner appointed by the prime minister to oversee investigatory powers under Section 227. Adrian Fulford, an appeals court judge, was appointed to the role in March 2017.[170] The law includes some other safeguards, such as "double-lock" interception warrants. These require approval from both the relevant secretary of state and an independent judge, though the secretary alone can approve urgent warrants. Under Section 32, urgent warrants last five days; others expire after six months unless renewed under the same double-lock procedure. The act allows authorities to prohibit telecommunications providers from disclosing the existence of a warrant. Intercepting authorities that may apply for targeted warrants include police commissioners, intelligence service heads, and revenue and customs commissioners.[171] Applications for bulk interception, bulk equipment interference, and bulk personal dataset warrants can only be made to the secretary of state "on behalf of the head of an intelligence service by a person holding office under the Crown" and must be reviewed by a judge.

Bulk surveillance is an especially contentious issue in the UK because intelligence agencies developed secret programs under older laws that bypassed oversight mechanisms and possible means of redress for affected individuals. These programs affected an untold number of people within the UK, even if they were meant to have only foreign targets. Tempora, a secret surveillance project documented in the Snowden leaks, is one example. A number of other

legislative measures authorized surveillance,172 including RIPA.173 RIPA was not repealed by the IP Act, though many of its competences were transferred to the newer legislation. A clause within Part I of RIPA allowed the foreign or home secretary to sign off on bulk surveillance of communications data arriving from or departing to foreign soil, providing the legal basis for Tempora.174 Since the UK's fiber-optic network often routes domestic traffic through international cables, this provision legitimized mass surveillance of UK residents.175 Working with telecommunications companies, GCHQ installed interception probes at the British landing points of undersea fiber-optic cables, giving the agency direct access to data carried by hundreds of cables, including private calls and messages.176

The Investigatory Powers Tribunal was established under RIPA to adjudicate disputes regarding government surveillance. In 2015, it found procedural irregularities in the retention of communications intercepted from Amnesty International and the South Africa–based Legal Resources Center, though it concluded that the interceptions themselves were lawful.177 In early 2016, the tribunal ruled that computer network exploitation carried out by GCHQ was in principle lawful within the limitations in the European Convention on Human Rights.178 The tribunal also noted that network exploitation is legal if the warrant is as specific and narrow as possible.

In July 2016, the Investigatory Powers Tribunal found that bulk data collection by GCHQ and two other intelligence agencies known as MI5 and MI6 was unlawful from March 1998 until the practice was disclosed in November 2015.179 The practice had been authorized under Section 94 of the Telecommunications Act 1984, which the Interception of Communications Commissioner described in June 2016 as lacking "any provision for independent oversight or any requirements for the keeping of records."180 The tribunal also said that the use of bulk personal datasets by GCHQ and MI5, commencing in 2006, was likewise unlawful until disclosed in March 2015. The datasets contained personal information that could include financial, health, and travel data as well as communications details.181 There were hearings in June and October 2017 on the process and legality of collecting and sharing these datasets.182

UK authorities have been known to monitor social media platforms.183 In London, for example, police reportedly monitored nearly 9,000 activists from across the political spectrum—many of whom had no criminal background—using geolocation tracking and sentiment analysis of data scraped from Facebook, Twitter, and other platforms.184 This information was then compiled in secret dossiers on each campaigner. In another example, the Online Hate Speech Dashboard, a joint project led by the National Online Hate Crime Hub of the National Police Chiefs' Council and Cardiff University, received £1 million ($1.3 million) in 2018 to use artificial intelligence for real-time monitoring of social media platforms meant to identify hate speech and "preempt hate crimes."185

C6 1.00-6.00 pts0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	3.003 6.006

Companies are required to capture and retain user data under certain circumstances, though the government issued

regulatory changes in 2018 to address flaws in the existing rules. While the government has legal authority to require companies to assist in the decryption of communications, the extent of its use and efficacy in practice remains unclear.

The UK has incorporated the GDPR into domestic law through the Data Protection Act 2018.186 Therefore, even once the post-Brexit arrangements are finalized, the GDPR in its entirety will continue to regulate data protection within the UK.

The government's response to the COVID-19 pandemic involved subscriber data obtained from telecommunications providers. In March 2020, mobile network O2 confirmed that it was providing anonymized aggregate location data from smartphones belonging to subscribers so that the government could monitor trends in compliance with social distancing guidelines.187

Data retention provisions under the IP Act allow the secretary of state to issue notices requiring telecommunications providers to capture information about user activity, including browser history, and retain it for up to 12 months. The Data Retention and Investigatory Powers Act 2014 (DRIPA), the older law this requirement was modeled on, was ruled unlawful in the UK and the EU in 2015.188 In January 2018, the Court of Appeal described DRIPA as being inconsistent with European law, since the data collected and retained were not limited to the purpose of fighting serious crime.189 In April 2018, the High Court ruled that part of the IP Act's data retention provisions similarly violated EU law, and that the government should amend the legislation by November 2018.190

In response, the government issued the Data Retention and Acquiring Regulations 2018, which entered into force in October 2018. The regulations limited the scope of the government's collection and retention of data and enhanced the transparency of the process.191 Furthermore, a newly created Office for Communications Data Authorisations would oversee data requests and ensure that official powers are used in accordance with the law.

Another problematic provision of the IP Act enables the government to order companies to decrypt content, though the extent to which companies would be willing or able to comply remains uncertain (see C4).192 Under Section 253, technical capability notices can be used to impose obligations on telecommunications operators both inside and outside the country "relating to the removal … of electronic protection applied by or on behalf of that operator to any communications or data," among other requirements. The approval process for issuing a technical capability notice is similar to that of an interception warrant.193 In March 2018, after consultations with the industry and civil society groups,194 the government issued the Investigatory Powers (Technical Capability) Regulations 2018, which governs how the notices are issued and implemented.195 The regulations specify companies' responsibilities in ensuring that they are able to comply with lawful warrants for communications data.

C7 1.00-5.00 pts0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	4.004 5.005

There were no reported instances of violence against internet users in reprisal for their online activities during the coverage period, though cyberbullying, particularly harassment of women, is widespread.196 A recent study found that one in three female members of Parliament had experienced online abuse, harassment, or threats.197 Online harassment of Muslims and other minorities is also a significant problem.198

The online harassment environment in the UK worsened during the COVID-19 pandemic, particularly for women and people of Chinese descent. Support services reported a surge in reports of cyberstalking and online harassment.199 Racist incidents involving people of Chinese or other Asian descent were reported throughout the UK, including several cases involving social media.200

A 2017 study found an increase in abusive comments targeting politicians on Twitter, which peaked on the day of the 2016 Brexit referendum.201 News reports indicated that hate crimes against minorities increased after the vote to leave the EU, which was driven in part by campaigns that depicted immigration as a threat to the British way of life. However, a 2016 analysis of cyberbullying in different parts of the UK found that regions with high levels of online hate speech or racial intolerance did not necessarily vote in favor of Brexit, and concluded that other issues were also driving the trend.202

C8 1.00-3.00 pts0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	2.002 3.003

Nongovernmental organizations, media outlets, and activists are generally not targeted for technical attacks by government or nonstate actors. Financially motivated fraud and hacking continue to present a challenge to authorities and the private sector. Cyberattacks have increased in recent years, and observers have questioned the security of a trend in which various machines, appliances, and objects are connected to the internet, creating what is known as the Internet of Things.203 During 2018, nearly 70 percent of companies and other commercial entities in the UK are reported to have been affected by cyberattacks.204

In March 2019, the information systems of the Police Federation of England and Wales were infected with ransomware—malicious software that blocks access to the contents of a computer or network and demands a ransom payment for access to be restored.205 The federation said there was no evidence that any information was leaked, although its data back-ups were deleted and other information was rendered inaccessible.206 The attack was limited to the federation's headquarters in Surrey and did not spread to its 43 associated offices.

In May 2017, the National Health Service suffered a ransomware attack affecting 40 organizations, effectively barring workers from patient case files.207 The attack had severe consequences, delaying or denying essential services for vulnerable individuals.208

During the 2019 election, the opposition Labour Party was subject to multiple cyber attacks, including a denial of

service and a leak of donor identities.[209] These attacks were not attributed to state actors and the party received ongoing support from the National Cyber Security Centre.