HICKMAN&ROSE
SOLICITORS

Smart devices and domestic abuse – a new battlefield or simply new weapons?

To some who are unhappy after the breakdown of a relationship, tracking a former partner's movements and online communications, altering the temperature in their home and making their doorbell repeatedly and inexplicably ring may seem an inconsequential form of retribution. Unfortunately, this type of behaviour has become more common. Individuals working with victims of domestic abuse report that some people are manipulating internet-connected devices such as phones, thermostats and security cameras to toy with current or former partners.

Victims can find their home devices turn against them, from speakers that blast noise of their own volition to showers that turn on by themselves. Additionally, some individuals have used spyware to access a partner's call logs, texts, GPS data, or their phone's built in camera and microphone.

Concern about this trend feeds into fears that the law is failing to catch up with changing technology, leaving victims unprotected. In fact, the criminal law is clear in its prohibition of certain behaviours. Legislation exists to prosecute even the most imaginative abuse.

Current legislation

Controlling or Coercive Behaviour

Individuals who use smart technology to distress and control their partner could potentially commit an offence of controlling or coercive behaviour. Statutory Home Office guidance published in 2015 states that this offence is a "purposeful pattern of behaviour which takes place over time in order for one individual to exert power, control or coercion over another".

Controlling behaviour is defined as "a range of acts designed to make a person subordinate and/or dependent" and coercive behaviour is "a continuing act or pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten".

The Home Office guidance gives examples of the kinds of behaviour that might be covered by this offence including: "monitoring a person via online communication tools or using spyware", "monitoring their time" and "taking control over aspects of their everyday life". Clearly, taking control of the front door security camera or of the temperature or lighting in a person's home could fall within this behaviour. For the offence to have been committed, four conditions must be met:

First, the controlling or coercive behaviour must take place repeatedly or on an ongoing basis. While each case will be considered individually, the courts may look for evidence of a pattern of behaviour established over time, rather than isolated incidents. For this reason, a person whose only wrongdoing is to gain unauthorised access to his or her partner's phone once or twice may not commit the offence but unauthorised access over a period of time, using the information they find to monitor and cause distress to their partner, may do.

Second, the pattern of behaviour must have a serious effect on the victim. The victim must fear that violence will be used against them on at least two occasions, or have been caused serious alarm or distress which has a substantial adverse effect on their usual day-to-day activities. What constitutes a substantial adverse effect may include a change in the victim's domestic routine and situations where the victim puts in place measures in their home to safeguard themselves, possibly including replacing smart devices.

Third, the behaviour must be such that the perpetrator knows or ought to know that it will have a serious effect on the victim.

Fourth, the perpetrator and victim have to be "personally connected" when the incidents take place. This covers those who are in an intimate personal relationship, family members who live together and people still living together who used to be in an intimate relationship. Crucially, the offence will not apply where ex-partners were living apart at the time of the behaviour or where the perpetrator has never been in a relationship with the victim. In these cases, harassment and stalking offences could potentially apply.

Harassment and Stalking

Offences of harassment and stalking are set out in the Protection from Harassment Act 1997. CPS guidance, published in 2018, makes clear that a very wide range of behaviour is capable of constituting harassment or stalking and recognises that both offences can take place online.

Harassment can include conduct that causes the victim alarm or distress or that puts people in fear of violence. The conduct must occur on at least two occasions to amount to a "course of conduct". The accused must know or ought to know that his or her conduct amounts to harassment. CPS Guidance states that there needs to be evidence that the conduct was targeted at an individual, calculated to cause them alarm or distress and that it was oppressive and unreasonable.

There is the simple offence of stalking and a more serious offence of stalking involving fear of violence or serious alarm or distress. Both are relatively new and only apply to behaviour after 25 November 2012. For the simple offence to have been committed, there needs to have been a course of conduct amounting to harassment which can be described as stalking. Although there is no strict legal definition of stalking, examples could include spying on someone, monitoring their use of the internet or any other form of electronic communication, or forcing contact with the victim through "any means". It is likely that manipulating the sound, lighting or temperature in the victim's home could be viewed as "forcing contact". A police officer who has reasonable grounds to believe a stalking offence may have been committed has the power to enter and search premises and seize items such as laptops and phones likely to be crucial to proving the suspect has interfered with the victim's devices.

For the more serious offence to have been committed, the stalking must either cause the victim to fear on at least two occasions that violence will be used against him or her, or cause serious alarm or distress which has a "substantial adverse effect" on the victim's usual day-to-day activities. According to the CPS guidance, the victim placing additional security measures in their home or changing the way they socialise may be evidence of a substantial adverse effect. Prosecutors will look at the cumulative effect of the ex-partner's behaviour.

Unauthorised Access

The Computer Misuse Act 1990 (CMA 1990) may apply to situations where a current partner, rejected suitor or ex-partner gains unauthorised access to their target's phone or computer. The offence contained within section 1 of CMA 1990 can apply whether or not the perpetrator then goes on to use this access to manipulate other internet-connected devices in the target's home. Unauthorised access to someone's social media accounts or hacking into someone's smart phone in order to access footage captured by their home security cameras could potentially fall within this offence.

Downloading spyware onto a partner's phone and using it to read their texts could also potentially amount to an offence of unlawful interception.

Anyone who gains unauthorised access to their target's mobile phone camera or webcam and publishes the footage online, risks committing a "revenge porn" offence if the footage could be deemed to be a private sexual film. The offence would also apply where the perpetrator accesses and publishes private sexual photos stored on the victim's phone or laptop.

Restraining Orders

Following criminal proceedings, protection could potentially be obtained through a restraining order. A restraining order can be made either upon application by the prosecutor or of the court's own volition after the perpetrator has been convicted or acquitted of a criminal offence. Such an order, intended to be preventative, not punitive, will be made if the court believes on the balance of probabilities that an order is necessary to protect the person named in it from harassment (if post-acquittal) and/or from conduct that will put them in fear of violence (if post-conviction). The court can hear evidence that may not have been admissible in the criminal proceedings, such as hearsay evidence or material covered in incident reports. Drafting a restraining order requires considerable thought: its terms must be sufficiently specific, clear, concise, reasonable and proportionate. The maximum sentence for breach of a protective order is 5 years' imprisonment.

Is legislative change necessary?

While not every snooping partner will have committed an offence, the existing criminal law captures a wide range of behaviour related to the manipulation of someone else's smart devices. There does not seem to be a need for more legislation, more a requirement for the current legislation to be applied to new types of behaviour.

What else can be done?

Companies selling smart technology will likely come under increasing pressure to ensure their customers understand how to prevent and detect interference with smart devices. Ensuring that customers know how to reset systems, install updates and conduct security sweeps could save potential victims from unwanted interference further down the line.

University College London has recently published a list of resources to better inform and guide victims of technology-facilitated abuse[1]. The list provides useful information to understand how connected devices work, as well as tools to protect against unwanted intrusion.

By Rose Commander, solicitor and higher court advocate in the general crime department at Hickman & Rose.

This article was originally published in The Robotics Law Journal on 19 November 2018: http://www.roboticslawjournal.com/analysis/smart-devices-and-domestic-abuse-a-new-battlefield-or-simply-new-weapons-41033630

Return to Hickman & Rose Analysis: https://www.hickmanandrose.co.uk/site/about/analysis/

[1] https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/g-iot-resource-list