LIBERTY

PRIVACY INTERNATIONAL

NEIGHBOURHOOD WATCHED

How to oppose police surveillance in your local community

Campaign Pack





CONTENTS

ABOUT NEIGHBOURHOOD WATCHED 3

KEY PRINCIPLES 4

THE WEB OF POLICE SURVEILLANCE 5

- Facial recognition 6
- Mobile phone extraction 6
- Predictive policing 7
- Body worn video cameras 7
- Social media intelligence 7
- IMSI catchers 8
- Hacking 8

WHAT YOU CAN DO: INFORM, EMPOWER, MOBILISE 9

OUR CAMPAIGN GOALS 10

WHAT ARE POLICE AND CRIME COMMISSIONERS? 11

- What is a Police and Crime Panel? 12
- Why contact your PCC? 12
- Taking action 12

YOUR PCC 13

- Who is my PCC? 13
- What party is my PCC a member of? 13
- What issues are important to them? 13
- What have they said in the past on this issue or similar issues? 13

HOLD A COMMUNITY MEETING 14

- Create your list of demands 14
- Where do I start? 14
- What do you need? 14
- How will the meeting work? 14
- What do you want to achieve? 14

YOUR LIST OF DEMANDS 15

NEXT STEPS 16

ABOUT US 17



ABOUT NEIGHBOURHOOD WATCHED

Police are rolling out new surveillance technologies which put our rights at risk – including our rights to privacy, free speech, freedom of association and freedom from discrimination.

From facial recognition and social media monitoring to hacking us and examining our mobile phones, UK police forces can watch and keep tabs on us as we go about our everyday lives on a scale not previously possible. Despite these developments, there is a lack of transparency and debate about their use of new tech.

The police are not open and honest with the public about what technology they use, where they use it, which communities they use it against and what laws allow them to do so. They will frequently deploy these tools without public consultation, without your consent or knowledge and often with no clear legal basis.

These technologies can be used to target, profile and discriminate against certain communities – including people from minoritised ethnic groups, unwaged or low-income groups, and those who are politically active.

That's why local elected representatives such as Police and Crime Commissioners (PCCs –see page 11 for more information) must do more. They need to take an active role to protect people's rights and ensure policing in the modern era is accountable, with strict safeguards in place to prevent abuse of power and key impact assessments completed before these tools are rolled out and it's too late.

We want to shine a light on tech where there has been a disappointing lack of transparency from the police and inadequate scrutiny. We want you to have a say on whether your local police force should buy or use highly invasive surveillance tools. And we want you to put pressure on PCC's to do their job.

It is vital we all act now.

Demand transparency. Stop unaccountable and unlawful police surveillance. ***Protect your neighbourhood from being watched.***

These technologies can be used to target, profile and discriminate against certain communities



KEY PRINCIPLES

- Local communities should be informed about police use of surveillance technologies and given the opportunity to scrutinise them.

- Before any decision to buy, trial or use surveillance tech, the police must carry out and publish human rights impact assessments and hold public consultations to seek the views of the local community.

- Local police forces should produce annual reports on their use of surveillance technology – including how it has been used, any misuse or errors and how it has affected people's rights.

- Police forces should provide the following information as part of their consultation with local communities:
  - How the technology works
  - What it costs
  - How it will be funded
  - The legal basis for use
  - What codes and guidance regulate its use
  - How it affects your rights
  - How your personal data will be used
  - What safeguards will be put in place
  - What impact assessments have been carried out
  - What independent oversight exists

- Information about police surveillance technology should be made public and should be written in a clear and concise way.

THE WEB OF POLICE SURVEILLANCE



BODY WORN VIDEO CAMERAS



IMSI CATCHERS



MOBILE PHONE EXTRACTION

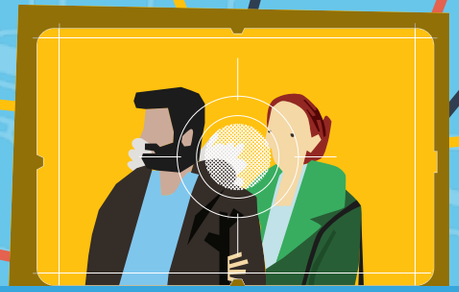




SOCIAL MEDIA INTELLIGENCE



PREDICTIVE POLICING



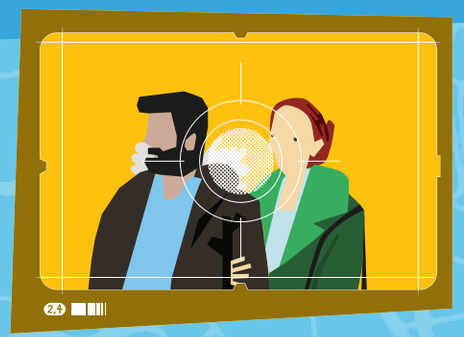
FACIAL RECOGNITION



HACKING

FACIAL RECOGNITION

- Facial recognition cameras capture live images of anyone walking past and take a unique ‘biometric’ map of your face – more like a fingerprint than a picture.
- UK police forces use facial recognition technology on our streets, at events and even at protests – even though it’s not clear what laws allow them to do so.
- The cameras can track and analyse people in public places in real time.
- Police check facial images against watch lists they put together, which may include people who have done nothing wrong. For example, they have used facial recognition cameras to target people with mental health conditions.
- Research has shown facial recognition technology to be biased against women and minoritised ethnic groups.
- As of summer 2019, the Information Commissioner – the UK’s data protection watchdog – is investigating the legality and effectiveness of live facial recognition. Police forces are also facing legal challenges for using it in public spaces.





MOBILE PHONE EXTRACTION

- Police can download all the data from your phone without your knowledge or consent.
- Mobile phones contain some of the most private information we store, including our messages, contacts, diaries, photos, videos, medical information, financial information and internet browsing history. Police can also download deleted data or data sent by secure messaging apps like WhatsApp.
- The data can go back years and relate to many people, not just the owner of the phone.
- Extraction software can also download data you have stored in the Cloud when you use apps like Uber, Amazon Echo and Google Home.
- Police need a warrant to search your home – but not your phone.

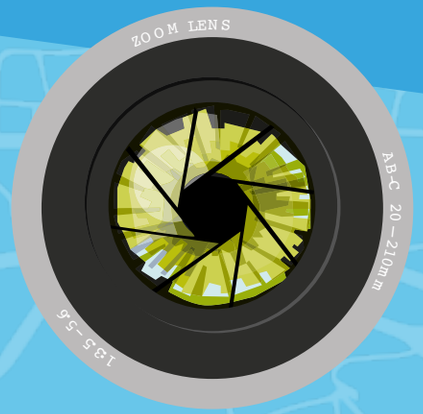


SOCIAL MEDIA INTELLIGENCE

- Whatever your privacy settings, the police can monitor and analyse your social media without you ever knowing – and they can do this on a mass scale.
- Your social media activity can be used to profile you, including determining your moods, opinions, activities, and relationships with others.
- Police officers might also pose as a new friend to access your social media profile – which is undercover police work being carried out without a warrant.
- These activities not only impact the people being monitored – everyone within a social network risks being caught in this web of surveillance.

BODY WORN VIDEO CAMERAS

- These cameras are worn by police officers and record video and audio from their perspective.
- They can generally be switched on and off at the officer's discretion and can be used as a form of surveillance and intelligence gathering.
- They can record in public and private spaces.
- Footage can be used with other tech like facial recognition to identify and track people in real time.
- 71 per cent of UK police forces use them, and every force in the country will have them by autumn 2019.





PREDICTIVE POLICING

- Predictive policing computer programs use personal and historical police data to predict where crimes might occur and who might commit them.
- The historical arrest data and other data held by the police will reflect long-standing bias. This means the program's predications will reflect pre-existing inequalities and the over-policing of marginalised communities.
- There is a lack of transparency around the use of these programs and it is very difficult to understand how these algorithm-driven predictions are made – making it near-impossible to challenge the decisions they make.

IMSI CATCHERS

- IMSI catchers imitate mobile phone signal towers and trick phones into connecting with them, allowing the police to covertly locate, track and collect data from devices in a broad geographic area.
- IMSI catchers snatch a phone's IMSI number. IMSI numbers are found on individual SIM cards, and can be used to identify the mobile phone user.
- IMSI catchers can also be used to intercept and monitor your calls and messages.
- Some IMSI catchers can manipulate the data people send or receive. You wouldn't even know it was happening.
- Although evidence shows police forces have purchased IMSI catchers, the police 'neither confirm nor deny' that they use them.



HACKING

- Remote hacking allows the police to access your internet-connected devices, including login details, passwords and internet browsing histories. They can also turn on your microphone, camera and GPS location tracking to monitor in real time.
- Police can exploit existing programming vulnerabilities to collect data and modify software. Instead of helping to fix flaws in our devices and networks, they leave them insecure and easy targets for criminals.



FIND OUT MORE

Read our short explainers and learn more at:

privacyinternational.org/campaigns/neighbourhood-watched libertyhumanrights.org.uk/stand-police-spying

WHAT YOU CAN DO



1. INFORM

Share knowledge with your friends, family and social media contacts to raise awareness about the intrusive technologies that the police are using in secret.

2. EMPOWER

Arm yourself with information in this Campaign Pack to ensure you understand what these technologies are, how they are used and how they pose a threat to your rights. Find out which technologies are being deployed in your local area so you know what the police are using to spy on your community. Discover if there are already local or nearby organised groups who could help support your campaign.

3. MOBILISE

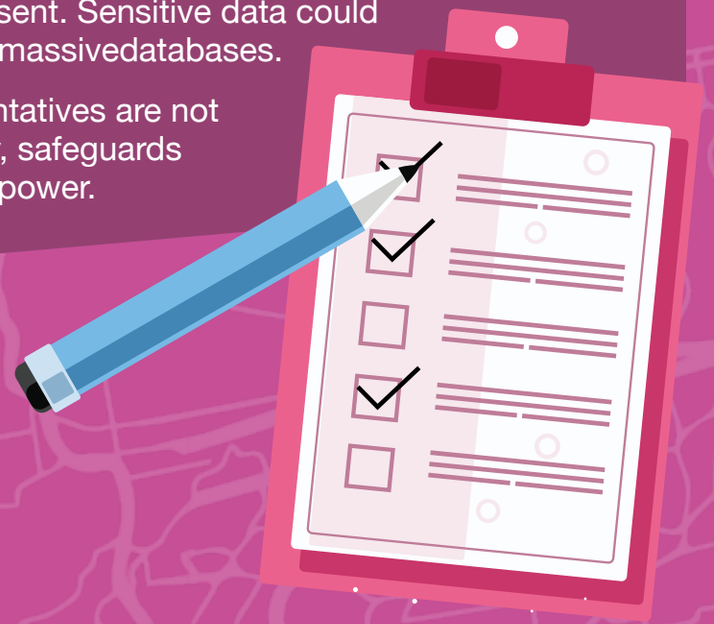
Organise a community action with people in your local area, and discuss ways to resist police surveillance tech together. This could include organising a meeting with your local Police and Crime Commissioner. See more details on this below.



OUR CAMPAIGN GOALS

1. Hold the police to account over the secretive roll-out of police spy-tech, and resist ever-present surveillance

- New technologies change the nature of policing from targeting individual suspects to giving officers the ability to monitor anyone, at any time, with the click of a button.
- The broad range of police tech, used together, creates a web of surveillance which may see barely noticeable but is hugely intrusive.
- This web includes biometric data, which can be taken without our knowledge or consent. Sensitive data could then be linked across massivedatabases.
- Local elected representatives are not ensuring transparency, safeguards and checks on police power.



2. Oppose policing which relies on data to create crude profiles of us

- The police have the capability to capture enormous amounts of data about us, cross reference it against other information and draw conclusions from it – sometimes using algorithms to make decisions about us.
- People are being targeted for “pre-criminality” and placed on databases such as the highly controversial and discriminatory Gangs Matrix.

3. Resist surveillance which is disproportionately targeted against minoritised communities

- Because surveillance technologies rely on biased data and lack public input, they disproportionately target minoritised communities.
- Predictive policing programs and algorithms, which feed off surveillance data, are not neutral – they worsen pre-existing bias and social inequality.

WHAT ARE POLICE AND CRIME COMMISSIONERS?

YOUR PCC

Find out who your PCC is at: apccs.police.uk/find-your-pcc/

There are 40 police forces across England and Wales, and each one has a Police and Crime Commissioner (PCC).

PCCs play a very important role in local policing. Their job is to be the voice of their local community and to hold the police to account. This means that they should listen to and represent your views about how the police work in your area – and this includes topics like police surveillance and new policing technologies.

PCCs are elected by the public in each local area. This means that people over 18 who are registered to vote can choose a PCC who has an approach to policing that they agree with.

The next elections for PCCs will be in 2020.

In Greater Manchester and London, the PCC's responsibilities are taken on by the Mayor, who is also elected.

Their job is to be the voice of their local community and to hold the police to account.

THE ROLE OF PCCs

PCCs often work with other organisations and agencies, at both a local and national level, to plan their approach to preventing and reducing crime. They might work with other PCCs and the Home Office to roll out new policing technology in your local area.

The key law which outlines the role of PCCs is called the Police Reform and Social Responsibility Act 2011. This Act states that it is the job of PCCs to:

- secure an efficient and effective police for their area;
- appoint the Chief Constable, hold them to account for running the force and if necessary dismiss them;
- set the police and crime objectives for their area through a police and crime plan;
- set the force's budget and determine how much money to raise from local residents through Council Tax; and
- bring together community safety and criminal justice partners, to make sure local priorities are joined up.

WHAT IS A POLICE AND CRIME PANEL?

Each policing area also has a Police and Crime Panel (PCP). The PCP challenges, scrutinises and supports the local PCC.

Each panel reviews police and crime plans, conducts hearings and deals with any complaints against the PCC. PCPs are made up of local councillors and 'lay members' (i.e. local people who are not politicians).

TAKING ACTION

Lobbying your PCC can include a number of actions, such as sending them letters, meeting with them, organising a rally or signing a petition.

The more people you encourage to contact your PCC about the same issue, the more likely they are to do something about it.

You can share your views on social media, use our online tool to contact your PCC or use this pack to help you organise a community meeting.

You can also go to one of your PCC's "surgeries". Some will be drop-in sessions, while others may require an appointment. Call your PCC's office to check what the process is in your local area and for future dates.



WHY CONTACT YOUR PCC?

The law says that the PCC must consider the opinion of local people when they develop policy. This also links with the PCC's legal obligation to make certain kinds of information public.

The PCP has no statutory role in consulting the public (unlike the PCC), but they can support the process of gathering public opinion. Police and Crime Commissioners are elected to hold your police force to account for delivering the kind of policing you want to see. Their aim is to cut crime and to ensure your police force is effective.

Anyone in your community – including you – can bring important issues to your PCC's attention. PCCs have the power to set police and crime plans and to ensure the budget is spent appropriately. Your PCC can also raise important questions with the Home Office about wider policy decisions.

So telling your PCC what issues your community is concerned about and what they can do to help is a crucial way of ensuring they are helping the people they serve.

YOUR PCC

Who is my PCC?

Find out who your PCC is at apccs.police.uk/find-your-pcc/. Here, you will also find a link to their individual website, where you can learn more about them, their plans and their priorities.

What issues are important to them?

What political party is my PCC a member of?

What have they said in the past about police use of tech or similar issues?

HOLD A COMMUNITY MEETING

Meeting with people face-to-face is a powerful campaigning tool, and one of the most effective ways to join together with your local community, raise awareness and let your local PCC know how you feel about police surveillance.

You may know people who are passionately campaigning against police surveillance, or people around you may have very little or no knowledge about what surveillance tech the police are rolling out. Either way, everyone can benefit from coming together to discuss this issue and plan to take positive action.

LIST OF DEMANDS

Where do I start?

You may already be aware of local campaigning groups in your area who you could work with to host a meeting – or perhaps you want to use a local community base, such as a school, college, community centre or library.

Every meeting will be different, but some things to think about include:

What do you need?

- What practical things do you need – like an accessible space to meet, a laptop, access to PowerPoint, tables and chairs, drinks and snacks, someone to take notes?
- How will you invite people to the meeting? Make sure you leave enough time for everyone to see posters, check social media etc.

How will the meeting work?

- Will you have a Chair who invites people to speak? Will it be a more informal discussion group? Will you invite local activists to speak about their work and share information before opening it out to attendees?

What do you want to achieve?

- Drawing up a list of shared demands can be challenging – are you prepared for disagreement and to find a compromise?
- Once you have your list of demands, how will you share them with your local PCC? Will you email or post them in, or will you arrange for a follow-up meeting where you invite your local PCC along to hear what your local community has to say about police surveillance?
- How will you follow up?



OUR LIST OF DEMANDS

1.

2.

3.

4.

5.

6.

7.

8.

NEXT STEPS

You've been vocal on social media, contacted your PCC, drawn up your list of demands and maybe even held a meeting. So what next?

- Contact other nearby groups for advice, support and solidarity. Other communities nearby might be organising against police surveillance technologies as well.
- If you think that the police or PCC are withholding any information, you can try using a Freedom of Information Act request to get it – for example if you wanted to ask for a copy of local force policy, notes of relevant meetings or specific contracts for the technology they are using. You can find out more about Freedom of Information Act requests at: https://www.gov.uk/make-a-freedom-of-information-request.
- If your PCC has been responsive, you will want to make sure you ask them to keep in touch and update you on what they do following your meeting.
- If you have attended a meeting, you can send a follow-up letter or email summarising what you discussed. This will keep your conversation fresh in their mind and remind them of any actions you have asked them to undertake.
- Contact Liberty / Privacy International to see if we can provide information to support your work from our own research. You can also let us know about any responses or meetings you have with your local PCC – we would love to hear about the impact you are having and your experiences can help inform our policy and campaigning work.

Download our Explainer PDFs

Facial Recognition

Mobile Phone Extraction

Social Media Intelligence

Body Worn Video Cameras

Predictive Policing

IMSI Catchers

Hacking

ABOUT LIBERTY / PRIVACY INTERNATIONAL

LIBERTY

Liberty is an independent membership organisation. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly.

We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account. We empower others to defend their own rights and the rights of their family, friends and communities.

Our principles are guided by evidence and expertise – not political agenda, profit or popular opinion. We're not afraid to speak uncomfortable truths or confront intolerance and abuse of power wherever we find it.

Together we've been making the UK a fairer, more equal place since 1934. Join us. Stand up to power.

https://www.libertyhumanrights.org.uk/

PRIVACY INTERNATIONAL

PI is a charity that challenges the governments and companies that want to know everything about individuals, groups, and whole societies.

The future PI wants is one where people are in control of their data and the technology they use, and governments and companies are no longer able to use technology to monitor, track, analyse, profile, and ultimately manipulate and control us. But we have to fight for that future.

Privacy International is fiercely independent and all our campaigns against companies and governments are driven solely by our charitable aims: to promote the human right of privacy throughout the world.

https://privacyinternational.org/