

【治理偷窥黑产之二】

非法使用窃听、窃照专用器材造成严重后果  
处二以下有期徒刑、拘役或者管制

# 在酒店非法安装摄像头 3名嫌疑人被逮捕



“偷窥”视频的背后是一条非法安装、上传、共享、买卖交易的黑色产业链，严重侵犯公民隐私权。专家指出，应采取技术措施与法律手段，斩断贩卖公民隐私的黑色产业链，不能让其成为个人隐私安全的隐患。《中华人民共和国刑法》第二百八十四条规定：非法使用窃听、窃照专用器材，造成严重后果的，处二以下有期徒刑、拘役或者管制。

## 案例1 “1个月能看5个房间” 他在多地宾馆安装摄像头

近日，上海市浦东新区检察院，以涉嫌非法使用窃听、窃照专用器材罪，对在酒店非法安装隐蔽摄像头、贩卖偷窥视频账号的3名犯罪嫌疑人批准逮捕。

付某从实体店购买了网络摄像头，然后自己去宾馆开房间安装。“我把摄像头的外壳拆掉，进房间后找宾馆隐蔽和方便取电的位置，一般是安装在宾馆房间里的空调上，然后连接宾馆的无线网络，这样网络摄像头就可以远程观看房间里的情况了。”

据付某供述，他在贵州、云南、四川等多地的宾馆里安装了摄像头，以每个120元或130元钱在网上售卖，成交后将二维码发给“顾客”扫码观看，获利1万余元。

柯某是付某的“顾客”之一，他从付某和他人处购买了数个账号。一次，柯某花了430元买了一个账号，可以在一个月内观看5个房间内的情况。可这个账号用了不到一个月就不能用了，于是柯某联系到了付某“维权”。

“那个账号被封了，你愿意的话帮我卖账号，我就免费给你几个号用。”在付某发出邀请后，柯某爽快答应了。于是他上家给的视频截图通过各类社交软件进行发布，吸引他人购买。据柯某供述：“上家给我的价格是一个账号180元，时效是一个月，可以看5个房间，我卖给下家的时候在200元到240元不等。”而根据酒店档次及房间内摄像头的角度，价格会有所不同。

为了扩大宣传吸引更多“顾客”，柯某在把自己购买的视频账号加价卖出后，以给予优惠为诱饵，让“顾客”帮忙宣传推广。其中一位“顾客”陈某，正巧欠了网贷无钱可还，他发现售卖偷窥视频账号来钱还挺快，于是加入了队伍，把从柯某处买的视频账号再加价卖给其他人，获利3000多元。

## 案例2 通过一款APP 控制18万个摄像头

西安的马先生不久前在客

厅安装了网络摄像头，以便能查看家中实时情况。但使用后不久，他发现摄像头在未进行任何操作的情况下，自己动了起来。这让他很意外，有种被偷窥的担忧。经过排查，朋友告诉他可能是手机上的软件密码被不法分子破解。

日前，在北京市第三中级人民法院审结的一起案件中，被告人巫某某通过一款APP控制了18万个摄像头，涉及众多私人住宅和公共场所。

据了解，“客户”可在该APP上付费注册会员，观看、保存摄像头拍摄的画面。该案中，巫某某用网购的黑客软件窃取某品牌网络摄像头的用户数据库，并通过社交媒体找技术人员开发违法APP。

无独有偶，2018年3月，丁某在QQ群里看到有人出售一款软件，能侵入他人摄像头，观看视频画面。丁某出于好奇，花钱购买了该软件。2019年5月31日至7月27日期间，丁某成功侵入367台网络摄像头并截取画面，供自己观看。

法院审理认为，丁某违反国家规定，对计算机信息系统实施非法控制，情节特别严重，已构成非法控制计算机信息系统罪。

## 案例3 借黑客软件非法控制 128台他人摄像设备

出于安全考虑，许多人装上智能摄像头以便实时查看家中情况。这也可能成为不法分子偷窥隐私的“猫眼”。近日，浙江省台州市黄岩区人民法院宣判一起非法控制计算机信息系统案件。

为了所谓的好奇心，2018年开始，杨某在网上学习用黑客软件控制摄像头偷窥隐私。

2019年3月，杨某购买了一个黑客软件，依照附赠的使用教程，他开始针对某品牌的网络摄像头进行破解扫描，其中没有更改过默认账号密码的网络摄像头会在列表中出现。借助黑客软件，杨某能获取列表中的摄像头画面，甚至可以调整摄像头监控角度。截至12月被查获时，杨某非法控制至少128台他人摄像设备，窥探陌生人的生活隐私，并下载了部分视频。

## 律师说法

### 买卖“偷窥视频”数据、 破解摄像头是否违法？

北京市安理律师事务所白小莉表示，破解他人安装在私人空间的摄像头的行为，属于违法行为。从民法角度而言，该行为很可能侵犯他人隐私权，以及侵害他人的个人信息，受害者可对破解者提起民事诉讼，要求赔偿损失和赔礼道歉。

关于隐私权，民法典第一千零三十二条规定：“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”。个人安装在私人空间的摄像头，所拍摄的内容很可能属于不愿为其他人所知晓的私密行为，属于个人隐私。如果破解他人安装在私人空间的摄像头，且摄像头所拍摄内容包含个人隐私的话，破解者就侵犯了他人的隐私权。

关于个人信息，民法典第一千零三十四条规定：“自然人的个人信息受法律保护”。破解他人安装在私人空间的摄像头所得到的画面，即使不包含个人隐私，也会有较大几率拍摄到个人面部信息，或言语交流中所包含的个人姓名、住址、电话号码、电子邮箱、健康信息、行踪信息等信息，上述内容都属于个人信息。所以，破解他人安装在私人空间的摄像头，破解者很可能会对他人的个人信息造成侵害。

### 不法分子破解他人摄像头 会受哪些处罚？

白小莉认为，从刑法角度

## 小贴士

### 如何提升摄像头安全性

普通消费者该如何提升摄像头的安全性，做到不被破解呢？

1.首先是路由器的安全，跟网络密码有关。摄像头一般自己也有一个密码，用户第一次安装的时候，设置一个复杂的密码，而且不要告诉外人；路由器的密码同样很重要，摄像头在路由器中有个固定的IP，如果别人通过密码破

而言，破解他人安装在私人空间的摄像头，并且非法获取个人隐私和个人信息，构成了非法控制计算机信息系统罪和侵犯公民个人信息罪，可数罪并罚。情节严重的，可处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，可处三年以上七年以下有期徒刑，并处罚金。“家庭摄像头用户被黑数据泄露，除了不法分子应该负责以外，摄像头设备厂商、云端运营商也需要负责。”

摄像头设备厂商、云端运营商如果没有立即采取补救措施，则应受到行政处罚；另外，无论摄像头设备厂商、云端运营商是否立即采取补救措施，受害人都可以要求其承担产品质量侵权责任。

### 商家销售偷拍设备 是否有法规约束？

白小莉表示，针孔摄像头、隐身摄像头属于窃听窃照间谍专用器材。销售针孔摄像头、隐身摄像头的行为，构成了非法生产、销售专用间谍器材、窃听、窃照专用器材罪；使用针孔摄像头、隐身摄像头的行为，构成了非法使用窃听、窃照专用器材罪。

《刑法》第二百八十三条规定：“非法生产、销售专用间谍器材或者窃听、窃照专用器材的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；情节严重的，处三年以上七年以下有期徒刑，并处罚金”。第二百八十四条规定：“非法使用窃听、窃照专用器材，造成严重后果的，处二年

以下有期徒刑、拘役或者管制”。

### 买卖“偷窥视频” 是否构成犯罪？

白小莉称，从民法视角下对他人隐私权和个人信息的侵害来看，买卖他人隐私视频的行为，同破解他人安装在私人空间的摄像头的行为一样，是对他人隐私权和个人信息的侵害，买卖双方都是受害人，受害者可向法院对买卖双方提起民事诉讼，要求赔偿损失和赔礼道歉。

从刑法角度而言，买卖他人隐私视频的行为，构成了侵犯公民个人信息罪，买卖双方都可以构成犯罪主体；同时，若隐私视频中包含淫秽内容，则卖方构成了制作、复制、出版、贩卖、传播淫秽物品牟利罪。

此外，构成侵犯公民个人信息罪的，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。构成制作、复制、出版、贩卖、传播淫秽物品牟利罪的，若隐私视频中包含淫秽内容，则卖方出售该隐私视频的行为很可能构成制作、复制、出版、贩卖、传播淫秽物品牟利罪。出售者将被处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

保存的视频清理掉。另外，视频监控软件要修改密码或者清除登录。

4.经常登录摄像头进行查看，如发现角度不对等情况，就需要警惕自己的账号安全。摄像头一定不要正对卧室、浴室等隐私区域，还要留意摄像头角度是否发生过变化，养成定期查杀病毒的好习惯。