# اگر کوئی ایجنٹ دستک دیتا ہے

centerforconstitutionalrights

*on the front lines for social justice*

# فہرست مشمولات


## تعارف 4

## ملاقاتیں اور تلاشیاں 6

اگر نفاذ قانون سے متعلق ایجنٹ کے ذریعہ مجھ تک رسائی ہوتی ہے یا مجھے طلب کیا جاتا ہے تو، کیا مجھے بات کرنا ضروری ہے؟ 6

اگر میں بات کرتا ہوں تو اس کے کیا نتائج برآمد ہوتے ہیں؟ 8

اگر کوئی ایجنٹ میرے گھر، اپارٹمنٹ یا دفتر کی تلاشی لینے کا مطالبہ کرتا ہے تو کیا ہوگا؟ 9

اگر میں آس پاس موجود نہیں ہوں اور ایجنٹ میرے کمرے کے / کی ساتھی سے میری املاک کی تلاشی لینے کو کہتا ہے تو کیا ہوگا؟ 10

کیا ایجنٹ میری ردی کی تلاشی لے سکتے ہیں؟ 10

اگر کوئی ایجنٹ وارنٹ یا گرانڈ جیوری کا پروانہ طلبی حاصل کرنے کی دھمکی دیتا ہے سوائے اس صورت کے کہ میں اس سے بات کروں یا تلاشی لینے کی منظوری دوں تو کیا ہوگا؟ 11

اگر کوئی ایجنٹ تلاشی کا وارنٹ موجود ہونے کا دعوی کرتا ہے تو کیا ہوگا؟ 11

ایجنٹ کو میرے کار کی تلاشی لینے سے باز رکھنے کے لئے مجھے کیا حقوق حاصل ہیں؟ 11

اگر میرے دفتر یا گھر میں توڑ پھوڑ ہوئی ہے اور مجھے شبہہ ہے کہ اس کا محرک خفیہ معلومات اکٹھا کرنا تھا تو مجھے کیا کرنا چاہیے؟ 12

اگر ایجنٹ مجھے گرفتاری کے وارنٹ دکھاتے ہیں تو مجھے کیا کرنا چاہیے؟ 13

اگر مجھے پروانۂ طلبی موصول ہوتا ہے تو مجھے کیا کرنا چاہیے؟ 14

## دخل اندازی اور انسانی نگرانی 16

خفیہ ایجنٹ اور مخبر جو کام انجام دے سکتے ہیں کیا ان کی کوئی تحدید ہے؟ 18

جال میں پھانسنا کیا ہے؟ 18

دخل اندازی کرنے کے کسی ایجنٹ کے اختیار پر کون سی دستوری تحدیدات لاحق ہیں؟ 19

میں دخل اندازی کے ثبوت کا تعین کس طرح کرسکتا ہوں؟ 20

میں اپنی تنظیم کو بچانے کے لئے کون سی احتیاطی تدابیر اختیار کرسکتا ہوں؟ 20

## الیکٹرانک نگرانی 22

### ٹیلیفون مواصلات

حکومت میری فون کالیں کب ٹیپ کرسکتی ہے؟ 22

اگر میرا فون ٹیپ ہو رہا ہے تو مجھے کیسے معلوم ہوگا؟ 24

متحرک وائر ٹیپ کیا ہے؟ 25

بگز کے بارے میں کیا خیال ہے؟ 25

فارن انٹلیجنس سرویلینس کورٹ اور نیشنل سیکیورٹی ایجنسی کی بلا وارنٹ وائر ٹیپنگ پروگرام کے بارے میں کیا خیال ہے؟ 26

سیلولر فونز، اسمارٹ فون اور PDAs میں سیکیورٹی کے کون سے خدشات لاحق ہوتے ہیں؟ 27

کیا حکومت میرے متنی پیغامات پر نگاہ رکھ سکتی ہے؟ 28

**انٹرنیٹ مواصلات**
کیا حکومت بتا سکتی ہے کہ میں کون سی ویب سائٹیں دیکھتا ہوں؟ 30
کیا مجھے غیر سرکاری اداروں کی جانب سے ہونے والی الیکٹرانک نگرانی کی بابت فکر مند ہونا چاہیے؟ 31

**الیکٹرانک سیکیورٹی**
ڈیٹا کی مرموزکاری 32
ای میل کی مرموز کاری 33
پاسورڈز 34
ویب براؤزنگ 34
اپنے انٹرنیٹ خدمت فراہم کنندگان کو جانیں 35
اینٹی اسپائی ویئر پروگرامز استعمال کریں 35
ڈیٹا سنبھال کر رکھنا اور حذف کرنا 35

**گرانڈ جیوری اور گرانڈ جیوری کی مزاحمت 37**
گرانڈ جیوری کیا ہیں اور فعالیت پسندوں کے لئے وہ کس قسم کے خطرات کے حامل ہوتے ہیں؟ 37
اگر کوئی فرد گرانڈ جیوری کا پروانۂ طلبی دکھاتا ہے تو مجھے کیا کرنا چاہیے؟ 38
اگر مجھے گرانڈ جیوری کا پروانۂ طلبی موصول ہوتا ہے تو مجھے کون سے اختیارات حاصل ہیں؟ 39
میں گرانڈ جیوری کے پروانۂ طلبی کو کس طرح کالعدم قرار دوں؟ 40
اگر میں گرانڈ جیوری کے پروانۂ طلبی کی تعمیل سے انکار کرتا ہوں تو کیا ہوتا ہے؟ 41
اگر میں گرانڈ جیوری کے پروانۂ طلبی کی تعمیل کرتا ہوں تو کیا ہوتا ہے؟ 41
گرانڈ جیوری کے بعد کیا ہوتا ہے؟ 42

**غیر ملکیوں کے لئے خصوصی طور پر زیر غور امور 43**
تقریر اور سیاسی وابستگیاں 43
تلاشیاں اور ضبطیاں 44
چپ رہنے کا حق 44

**اختتامیہ 45**

**اضافی وسائل 46**

**اعترافات اور انتسابات 48**

# تعارف

نفاذ قانون سے متعلق وفاقی ایجنسیاں جیسے فیڈرل بیورو آف انویسٹی گیشن (FBI) انتہا پسند اور ترقی پسند تحریکوں کو نشانہ بنانے کی ایک سیاہ تاریخ کی حامل رہی ہے۔ ان تحریکوں کے خلاف وہ جو بعض غلط حربے استعمال کرتی ہیں ان میں شامل ہیں: تنظیموں کی ساکھ کو نقصان پہنچانے اور ان کی اعمال میں خلل ڈالنے کے لئے دخل اندازی؛ ذرائع ابلاغ میں شائع ہونے والی غلط معلومات اور جھوٹی کہانیوں کی تشہیر کرنا؛ جعلی ثبوت تیار کرنا؛ اور فعالیت پسندوں کو خوف میں مبتلا کرنے کے لئے گرانڈ جیوری کے پروانۂ طلبی استعمال کرنا۔ آج کے دور کے فعالیت پسندوں کو نفاذ قانون سے متعلق وفاقی ایجنسیوں کے ذریعہ لاحق ہونے والے خدشات اور ان کی چالبازیوں کو ساتھ ہی بہترین تحفظ فراہم کرنے والے سیکیورٹی کے متعدد کلیدی طریق کار کوبھی لازمی طور پر جان لینا اور سمجھ جانا چاہیے۔

فعالیت پسندوں کو نشانہ بنانے کے لئے وفاقی ایجنٹوں کے پاس اپنے دائرہ اختیار میں بہت سارے وسائل ہوتے ہیں۔ یوں تو ان وسائل اور حربوں کو جان اور سمجھ لینا ضروری ہے، مگر یہ بھی لازمی ہے کہ آپ حکومت کی کسی نگرانی یا دخل اندازی کے خوف کے شبہے کو مسترد کردیں، جو سماجی بدلاؤ کی صورت میں آپ کو اور آپ کی تنظیم کو صرف مفلوج بنانے کا کام کرے گی۔ اگر حکومت
کے جبر کا خوف آپ کو منظم ہونے سے روکتا ہے تو، مجبور کرنے والے ایجنٹوں کو بغیر کسی کوشش کے ہی کامیابی حاصل ہوجائے گی۔

سنٹر فار کانسٹی ٹیوشنل رائٹس [Center for Constitutional Rights - CCR] نے FBI کے ایجنٹوں اور دیگر وفاقی تفتیش کاروں کے ذریعہ امکانی طور پر نشانہ بنائے جانے والے فعالیت پسندوں کو مشورہ فراہم کرنے کے لئے " اگر کوئی ایجنٹ دستک دیتا ہے" (If an Agent Knocks) نامی کتابچہ تیار کیا۔ 1989 میں، اگر کوئی ایجنٹ دستک دیتا ہے کا حقیقتا اجراء ہونے کے بعد سے، ملک بھر میں ترقی پسند فعالیت پسندوں کی برادری میں وسیع پیمانے پر اس کی نشر و اشاعت ہوئی ہے۔ یہ رہنما کتابچہ اصل ورژن میں شامل مقررہ وقت سے مبرا مشورہ اور قانون و نفاذ قانون کے وسائل کی موجودہ صورتحال کی عکاسی کرنے کے لئے جامع نوعیت کی تازہ کاری دونوں ہی چیزوں پر مشتمل ہے۔ اس تجدید شدہ شمارہ میں آج کی ٹکنالوجی، بشمول سیل فون، ای میل اور ویب براؤزنگ کی جامع گفتگو شامل ہے۔ اس رہنما کو حکومت کی چھان بین سے اپنی ذات کو اور دیگر فعالیت پسندوں کو تحفظ فراہم کرنے کے لئے درکار معلومات کے لئے اور جدوجہد جاری رکھنے کے واسطے خود کو بااختیار بنانے کے لئے ایک ماخذ کے طور پر استعمال کرنا چاہیے۔

ایک فعالیت پسند کی حیثیت سے کسی فرد کو جن متعدد صورتحال کا سامنا ہوسکتا ہے ان کے مدنظر ہم نے وسیع پیمانے پر سوالوں کے جوابات فراہم کرنے کی کوشش کی ہے۔ ہمیں امید ہے کہ افراد اور گروپ عملی جوابات فروغ دینے اور تیار کرنے کے لئے یہ پرچہ استعمال کریں گے – اگر کوئی ایجنٹ آپ کے دروازے پر دستک دیتا ہے۔

اس اشاعت میں مستقل طور پر اس بات کی تاکید

کی جاتی ہے کہ سارے معاملات میں پیشہ ورانہ قانونی مشورہ طلب کرنا چاہیے۔ سنٹر فار کانسٹی ٹیوشنل رائٹس کے پاس انفرادی جرائم سے متعلق نمائندگی فراہم کرنے کی لیاقت نہیں ہے۔

ہر ریاست میں بار ایسوسی ایشنز ہیں جو وکیل کے حوالے فراہم کرسکیں گے، جن میں سے چند تو پرو بونو سروسز خدمات فراہم کرسکتے ہیں۔ اگر آپ کے شہر میں نیشنل لایرز گلڈ (www.nlg.org) کا کوئی جزء ہے تو، وہ اکثر و بیشتر ایسے وکلاء کے حوالے فراہم کرسکتا ہے جنہیں اس کتابچہ میں نشان زد امور کو حل کرنے کا تجربہ ہوتا ہے۔

# ملاقاتیں اور تلاشیاں

اس کتابچه میں مذکور معلومات انتہائی اہم ہے: آپ کو خاموش رہنے کا حق حاصل ہے، اور عموما ایسا ہی کرنا بہتر خیال کیا جاتا ہے۔ ریاستہائے متحدہ کے دستور کی پانچویں ترمیم آپ کو نفاذ قانون سے متعلق ایجنسیوں کے سامنے خود کو ملزم قرار دینے والی معلومات کا افشاء کرنے پر مجبور کیے جانے سے تحفظ فراہم کرتی ہے۔

کرنے کے بجائے کہنا بہت آسان ہے۔ ایجنٹ تربیت یافته تفتیش کاران ہوتے ہیں؛ ان کے پاس استدلال کی قوت اور کسی فرد کو مبتلائے خوف، قصوروار ہونے یا معلومات حاصل کرنے کے لئے ان کی درخواستیں مسترد کرنے کی بے رخی کا احساس دلانے کی صلاحیت ہوتی ہے۔ ایک ایجنٹ یه کہه سکتا / سکتی ہے که ان سے بات کرنے پر رضامند نه ہونے کا مطلب یه ہوسکتا ہے که آپ لازمی طور پر کچھ چھپا رہے ہیں۔ وہ یه تجویز کرسکتا / سکتی ہے که وہ بس آپ سے چند سوالوں کے جوابات معلومات کرنا چاہتے / چاہتی ہیں اور اس کے بعد وہ آپ کو اکیلا چھوڑ دیں گے / گی۔ ایجنٹ وارنٹ حاصل کرنے کی دھمکی بھی دے سکتا / سکتی ہے۔

ایجنٹ کی دھمکیوں یا یقین دہانیوں کی وجه سے خوف میں مبتلا ہونے یا ساز باز کرنے کی ضرورت نہیں ہے۔ ہمیشه بہترین طریقه یہی ہوتا ہے که وکیل کی موجودگی کے بغیر بات نه کی جائے۔ اگر آپ بات کرلیتے ہیں تو آپ کی کہی ہوئی کوئی بھی بات آپ کے اور دوسروں کے خلاف استعمال ہوسکتی ہے۔ حتی که اگر آپ پوری سچائی بتا دیتے ہیں، اور اگر ایجنٹ کو آپ کے اوپر یقین نہیں ہوتا ہے تو، وہ آپ کو ایک وفاقی آفیسر کے سامنے جھوٹ بولنے کا الزام عائد کرنے کی دھمکی دے سکتا / سکتی ہے – جو که ایک حقیقی جرم ہے۔

**اگر نفاذ قانون سے متعلق ایجنٹ کے ذریعه مجھ تک رسائی ہوتی ہے یا مجھے طلب کیا جاتا ہے تو، کیا مجھے بات کرنا ضروری ہے؟**

خاموش رہنے کا اپنا اراده پوری طرح سے واضح کردیں۔ کہدیں که "میں آپ سے بات نہیں کر رہا ہوں"، یا "میں آپ سے کچھ بھی کہنے سے قبل اپنے وکیل سے بات کرنا چاہوں گا۔" آپ یه بھی کہه سکتے ہیں که "مجھے آپ سے کچھ بھی نہیں کہنا ہے۔ میں اپنے وکیل سے بات کروں گا / گی اور انہیں آپ سے رابطه کرنے کو کہوں گا / گی۔" آپ کو ایجنٹ سے بزنس کارڈ طلب کرنا اور یه کہنا چاہیے که آپ اپنے وکیل کا رابطه ان سے کروائیں گے۔ اس کے بعد سوالات پوچھنے کا سلسله ختم ہوجانا چاہیے۔

اس اصول میں صرف ایک استثناء اس صورت میں ہے جب آپ "رکیں اور شناخت کروائیں" والی کیفیت میں ہوں۔ سبھی ریاستیں آپ سے یه تقاضه کرتی ہیں که اگر گاڑی چلاتے ہوئے آپ کو اس سے اتار لیا جاتا ہے تو آپ سے ڈرائیور کا لائسنس دکھانے کو کہا جاتا ہے، اور سپریم کورٹ

(عدالت عظمی) نے ایسے قوانین وضع کر رکھے ہیں جو آپ سے بنیادی شناختی معلومات بیان کرنے کا مطالبہ کرتے ہیں، جیسے آپ کا نام اور پتہ معلوم کرنا ملزم قرار دینے والا عمل نہیں مانا جاتا ہے اور نفاذ قانون سے متعلق ادارے آپ سے اس طرح کی معلومات طلب کرسکتے ہیں۔ مگر وہ اس طرح کی معلومات صرف آپ سے ہی طلب کرسکتے ہیں، تاہم، صرف اس صورت میں جب آپ ایسی ریاست میں ہوں جہاں رکیں اور شناخت کروائیں والی کیفیت ہو۔ آپ کی ریاست میں موجود کوئی فعالیت پسند وکیل آپ کو بتاسکے گا کہ آیا آپ کی ریاست رکیں اور شناخت کروائیں والی کیفیت کی حامل ہے۔

اگر کوئی ایجنٹ فون پر کال کرتا ہے تو بھی انہی بنیادی اصولوں کا اطلاق ہوتا ہے۔ آپ کو کسی بھی ایسے ایجنٹ سے بات کرنا ضروری نہیں ہے جو غیر متوقع طور پر آپ کو کال کرتا ہے۔ یہ حقیقت پر مبنی نہیں بھی ہوسکتا ہے۔ اپنے آپ کو نفاذ قانون سے متعلق بتانے والے کسی بھی فرد کو آپ بتا دیں کہ آپ کا وکیل انہیں واپسی کال کرے گا – اس کے بعد ان سے بات کرنا بند کردیں۔

اگر ممکن ہو تو، ایجنٹ کا نام، ٹیلیفون نمبر اور ایجنسی کا پتہ معلوم کرلیں۔ یہ چیز ان کے بزنس کارڈ پر درج ہونی چاہیے، یا انہیں یہ معلومات فراہم کرنے پر رضامند ہونا چاہیے۔ ایجنٹ کے وہاں سے جانے اور رخصت ہونے کے فورا بعد اس باہمی تعامل کے بارے میں اپنی کوشش کی حد تک زیادہ سے زیادہ تفصیلات تحریر کرلیں۔ یہ معلومات وکیل کے لئے اور ان دیگر افراد کے لئے بھی کارآمد ہوگی جن سے نفاذ قانون سے متعلق اہلکار نے رابطہ کیا ہوا ہے۔ کوشش کریں کہ ایجنٹ (ایجنٹوں) کا نام اور ان کی جسمانی ساخت؛ ایجنٹ جو کار چلا رہا تھا / رہی تھی اس کی ساخت؛ پوچھے جانے والے سوالات اور باہمی تعامل کے دوران ہونے والے تبصرے؛ روبرو ہونے کا وقت اور مقام؛ اور کسی گواہ کے رابطے کی معلومات تحریر کرلیں۔

عام طور پر بہترین طریقہ یہ ہوتا ہے کہ کسی وکیل کو شریک کیا جائے۔ وکیل آپ کے حقوق کو تحفظ فراہم کرتے ہوئے آگے کی کارروائی سے متعلق مشورہ دے سکتا ہے۔ وکیل ایجنٹ سے بات کرسکتا ہے؛ پتہ لگا سکتا ہے کہ چھان بین کس چیز کے بارے میں ہے؛ کسی قسم کی جرح سے تعلق رکھنے والے امور پر پابندیاں عائد کرنے کی کوشش کرسکتا ہے؛ اور آپ سے جرح ہونے کے وقت آپ کو مشورہ اور تحفظ فراہم کرنے کے لئے وہاں پر حاضر رہ سکتا ہے۔ کبھی کبھی وکیل کی جانب سے کی جانے والی ایک کال ہی ایجنٹ کو واپس ہوجانے پر مجبور کردیتی ہے۔

وکیل کے مشورے سے، آپ رو برو ہونے کے اس وقوعہ کی تشہیر ان دیگر افراد کے سامنے کرسکتے ہیں جو کسی چھان بین سے متاثر ہوسکتے ہیں۔ اگر فعالیت پسندوں کو معلوم ہے کہ چھان بین ہوئی ہے تو، وہ آپ کے حقوق کو تحفظ فراہم کرنے میں کافی زیادہ چوکسی برت سکتے ہیں۔ انتظام و انصرام اور عوامی دباؤ خوف میں مبتلا کرنے اور جال میں پھانسنے کے قیاسات کو منظر عام پر لاسکتا اور اس پر پابندی عائد کرسکتا ہے۔

1. ی اشاعت کے وقت، درج ذیل ریاستوں میں رکیں اور شناخت کروائیں وال کیفیت کے بعض طریقے رائج ہیں: الباما، اریزونا، ارکنساس، کولیراڈو، ڈیلیورے، فلوریڈا، جارجیا، الینوائس، انڈیانا، کنساس، لوئیسیانا، مسوری، مونٹانا، نبراسکا، نیویڈا، نیو ہیمپشائر، نیو میکسیکو، نیو یارک، نارتھ ڈیکوٹا، اوہیو، روڈ آئلینڈ، اوٹاہ، ورمونٹ اور وسکانسن۔

## اگر میں بات کرتا ہوں تو اس کے کیا نتائج برآمد ہوتے ہیں؟

جب آپ کو یہ لگے کہ ایجنٹ سے بات کرلینا دانشمندی ہے تو یہ صورتحال پیدا ہوسکتی ہے۔ شاید آپ کسی جرم کا شکار رہے ہوں یا آپ وفاقی حکومت کے ذریعہ مواخذہ کیے جانے والے دیوانی حقوق کی خلاف ورزی کا گواہ رہے ہوں۔

یہاں تک کہ ان حالات میں بھی آپ کو ایک وکیل موجود رکھنا چاہیے۔ وکیل یہ یقینی بناسکتا ہے کہ آپ کے حقوق تحفظ یافتہ ہیں جبکہ آپ کسی مخصوص وقوعہ سے تعلق رکھنے والی صرف لازمی معلومات ہی فراہم کریں۔ وہ گرانڈ جیوری کے سامنے گواہ کی موجودگی سے احتراز کرنے میں آپ کی مدد کرسکیں گے یا حاضری والے حالات کو قابو میں کرسکیں گے تاکہ کسی بھی فرد کے حقوق کے ساتھ جانبداری نہ ہونے پائے۔

اگر آپ سوالوں کے جوابات دینے کا ہی فیصلہ کرتے ہیں تو، آگاہ رہیں کہ سرکاری اہلکار کے سامنے جھوٹ بولنا بھی ایک جرم ہے۔ در حقیقت، کسی ایجنٹ کے سامنے بات نہیں کرنے کی ایک سب سے اہم وجہ یہی جرم ہے۔ ایک معیاری وفاقی نفاذ قانون سے متعلق اہلکار کی چالبازی یہ ہوتی ہے کہ حکومت کے لئے کسی مشتبہ یا محض مفاد کے حامل کسی فرد کے بارے میں حتی الامکان زیادہ سے زیادہ معلومات حاصل کی جائے۔ اس کے بعد نفاذ قانون سے متعلق وفاقی ایجنٹ بصورت دیگر کسی معمولی وقت پر جیسے ڈنر کے دوران یا بس بس اسٹاپ پر اس فرد کے پاس پہنچیں گے، اور اس فرد سے ایسے سوالات پوچھیں گے جن کا جواب انہیں پہلے سے معلوم ہوتا ہے۔

مثلا، ایک ایجنٹ آپ سے پوچھ سکتا ہے کہ آیا آپ اس فرد کو جانتے ہیں (جس کو ان کے علم کے مطابق آپ جانتے ہیں) یا آپ سے پوچھ سکتا ہے کہ آپ وقوعہ کے وقت موجود تھے (جہاں پر ان کے علم کے مطابق آپ موجود تھے)۔ اگر آپ غیر ارادی طور پر اس کا جواب "نہیں" میں دیتے ہیں تو، یہ ایک قابل مواخذہ وفاقی جرم ہے جس کے لئے پانچ تا آٹھ سال کی سزائے قید ہے۔ پوچھ تاچھ کی اس چالبازی کا انتہائی تکلیف دہ پہلو یہ ہے کہ بہت سارے افراد غیر ارادی طور پر اس وجہ سے سوالوں کا جواب نفی میں دیتے ہیں کہ وہ خوف زدہ یا بدحواس ہوتے ہیں۔ یہ حربہ ہر قسم کی چھان بین میں وفاقی تفتیش کاروں کے ذریعہ استعمال ہوتا ہے اور حالیہ دنوں میں فعالیت پسندوں کو نشانہ بنانے اور انہیں اپنے سابق رفقائے کار کے خلاف مخبر بن جانے کے لئے استعمال کیا گیا ہے۔

وفاقی افسر کے سامنے جھوٹ بولنا ایک وفاقی جرم ہے اور یہ صرف وفاقی ایجنٹوں کے ذریعہ پوچھے گئے سوالوں پر لاگو ہوتا ہے۔ تاہم، اس امر سے واقف رہیں کہ بعض مقامی اور ریاستی ایجنٹ، جیسے کسی شہر کی جوائنٹ ٹیررزم ٹاسک فورس کے ممبران کو بھی "وفاقی" ایجنٹ سمجھا جاتا ہے۔ ساتھ ہی، کچھ ریاستوں میں ریاستی افسر کے سامنے جھوٹ بولنا اسی طرح کے جرائم ہیں۔ محفوظ ترین انتخاب یہی ہے کہ نفاذ قانون سے متعلق اہلکار سے بات نہ کی جائے۔

اگر آپ سوالوں کا جواب دینا شروع کرتے ہیں تو، آپ کسی بھی وقت سوالوں کا جواب دینے سے انکار کرسکتے ہیں۔

## تلاشی کے وارنٹ

تلاشی کا وارنٹ عدالت کا فرمان ہوتا ہے جو نفاذ قانون سے متعلق اہلکار کو کسی مخصوص جائے وقوع کی تلاشی لینے اور شہادت ضبط کرنے کا اختیار عطا کرتا ہے۔

چوتھی ترمیم لوگوں کو نامناسب تلاشیوں کے خلاف تحفظ فراہم کرتی ہے۔ جب تک کسی استثناء کا اطلاق نہ ہوتا ہو، نفاذ قانون سے متعلق اہلکار کو تلاشی لینے کے لئے تلاشی کا وارنٹ حاصل کرنا ضروری ہوتا ہے۔ تلاشی کے وارنٹ کی تائید میں امکانی وجہ، نیز وارنٹ کے لئے درخواست دینے والے افسر کے ذریعہ حلفیہ بیان کردہ حقائق موجود ہونے چاہئیں۔ تلاشی کا وارنٹ تلاشی لیے جانے کی جگہ اور جس چیز (جن چیزوں) کی تلاشی لی جانی ہے ان کے ساتھ مخصوص ہونا چاہیے۔ اس پر جج کا دستخط ہونا چاہیے، حالیہ تاریخ درج ہونی چاہیے (جو دو ہفتوں کے اندر کی تاریخ ہو) اور اس مقام کا صحیح پتہ مذکور ہونا چاہیے۔

امکانی وجہ کا مطلب یہ ہے کہ اس امر کا تعین کرنے کے حقائق بہرحال موجود ہوں کہ جس جگہ کی تلاشی لی جائے گی وہاں پر شاید جرم کا ثبوت مل سکتا ہے۔ امکانی وجہ کی بنیاد حقائق پر ہونی چاہیے - صرف اٹکلیں کافی نہیں ہیں۔

تلاشی کے وارنٹ سے لیس، نفاذ قانون سے متعلق ایجنٹوں کے پاس آپ کی املاک کی تلاشی لینے کا حق حاصل ہوتا ہے۔ اگر آپ انہیں رسائی کی اجازت نہیں دیتے ہیں تو، وہ تلاشی کا عمل انجام دینے کے لئے شاید طاقت کا استعمال کریں گے۔

**ان کے وسائل کو جانیں**

## اگر کوئی ایجنٹ میرے گھر، اپارٹمنٹ یا دفتر کی تلاشی لینے کا مطالبہ کرتا ہے تو کیا ہوگا؟

نفاذ قانون سے متعلق اہلکار کو وارنٹ کے بغیر اپنی ذات یا املاک کی تلاشی ہرگز نہ لینے دیں۔ کچھ مخصوص محدود حالات کو چھوڑ کر، نفاذ قانون سے متعلق اہلکار کے پاس آپ کی املاک کی تلاشی لینے کے لئے وارنٹ ہونا لازمی ہوتا ہے۔ آپ سے صرف قانونی طور پر نفاذ قانون سے متعلق اہلکار کو اپنے گھر، دفتر یا دیگر نجی جگہ میں صرف اسی صورت میں داخل ہونے دینے کا تقاضہ کیا جاتا ہے جب ان کے پاس وارنٹ ہو۔

اگر آپ ایجنٹوں کو اجازت دیتے ہیں، ، تو وہ وارنٹ کے بغیر بھی آپ کے گھر کی تلاشی لے سکتے ہیں اور انہیں وارنٹ کے بغیر بھی تلاشیاں لینے کے لئے آپ کی منظوری حاصل کرنے کی تربیت ملی ہوتی ہے۔ ایسے سوالات سے چوکنا رہیں جو تلاشی کے لئے آپ کی منظوری حاصل کرنے کے واسطے تیار کئے گئے ہوتے ہیں۔ یہ سوالات غیر ضرر قسم کے ہوسکتے ہیں، مثلا "اگر میں اندر آؤں تو آپ کو برا تو نہیں لگے گا؟" بس کسی ایجنٹ کو اپنے گھر میں داخل ہونے دینا ہی پوری جگہ کی تلاشی کے لئے منظوری سمجھا جاسکتا ہے۔

قانونی طور پر، تلاشی کی درخواست کا بہترین جواب یہ ہے کہ "میں تلاشی لینے کی منظوری نہیں دیتا ہوں۔" یہ بات بلند آواز میں اور فخریہ طور پر کہیں تاکہ کوئی گواہ اسے سن سکے۔

## اگر میں آس پاس موجود نہیں ہوں اور ایجنٹ میرے کمرے کے /کی ساتھی سے میری املاک کی تلاشی لینے کو کہتا ہے تو کیا ہوگا؟

کمرے کا / کی ساتھی عمومی، مشترکہ جگہ اور خود اپنی جگہ کی تلاشی لینے کی اجازت دے سکتا / سکتی ہے۔ کمرے کا / کی ساتھی کسی مشترکہ مکان یا اپارٹمنٹ میں دوسرے فرد کی نجی جگہ کی تلاشی لینے کی منظوری نہیں دے سکتا / سکتی ہے۔ دوسرے لفظوں میں، کمرے کا / کی ساتھی آپ کے باورچی خانے، اقامتی کمرے یا مشترکہ غسل خانے کی تلاشی لینے کی اجازت دے سکتا / سکتی ہے، لیکن آپ کی نجی خوابگاہ کی نہیں، سوائے اس صورت کے جب آپ اس کے ساتھ اس کا اشتراک کرتے ہوں یا اس کا استعمال کسی اور طریقے سے مشترکہ طور پر ہوتا ہو۔

شریک حیات اپنے / اپنی ساتھی کے نجی کمروں کی تلاشی لینے کی اجازت دے سکتا / سکتی ہے کیونکہ انہیں گھر میں ساری ہی جگھوں پر مشترکہ اختیار کا حامل سمجھا جاتا ہے۔ اسی طرح، والدین اپنے بچوں کی نجی جگھوں کی تلاشی لینے کی اجازت دے سکتے ہیں۔ کل ملاکر، اگر آپ کمرے کے / کی ساتھی یا ساتھی کے ہمراہ خوابگاہ کا اشتراک کرتے ہیں تو، وہ اس جگہ کی تلاشی لینے کی منظوری دے سکتے / سکتی ہیں۔ خلاف مرضی تلاشیوں سے تحفظ کے لئے، یقینی بنائیں کہ نجی جگہ نجی ہی بنی رہے۔ اگر آپ کمرے کے / کی ساتھی کو اپنی نجی جگہ پر باہمی رسائی یا قدرت حاصل کرنے کی اجازت دیتے ہیں تو، وہ اس جگہ کی تلاشی لینے کی منظوری دے سکتے / سکتی ہیں۔ کمرے کے / کی ساتھی، دفتر کے / کی ساتھی کو اور کسی بھی ایسے فرد کو جس کے ساتھ آپ جگہ کا اشتراک کرتے ہیں بتا دیں کہ کسی بھی جگہ، خاص طور پر آپ کی نجی جگہ کی تلاشی لینے کی اجازت ہرگز نہ دیں۔

## کیا ایجنٹ میرے ردی کی تلاشی لے سکتے ہیں؟

جب آپ اپنا کوڑا کچرا اپنے گھر سے باہر ڈال دیتے ہیں تو، ایجنٹ کسی وارنٹ یا کسی اور قانونی بندش کے بغیر اس کی تلاشی لے سکتے ہیں۔ عدالتوں کے مطابق اپنے کوڑے کچرے سے آپ کا کوئی رازدارانہ مفاد وابستہ نہیں رہتا ہے کیونکہ آپ نے اسے عام جگہ کے حوالے کردیا ہے۔ کسی بھی اور سارے حساس دستاویزات کو ضائع کرنے سے قبل پھاڑ دیں یا بصورت دیگر انہیں تباہ کردیں۔

## اگر کوئی ایجنٹ وارنٹ یا گرانڈ جیوری کا پروانہ طلبی حاصل کرنے کی دھمکی دیتا ھے سوائے اس صورت کہ جب میں اس سے بات کروں یا تلاشی لینے کی منظوری دوں تو کیا ھوگا؟

وارنٹ یا پروانۂ طلبی حاصل کرلینے کی کسی ایجنٹ کی دھمکیوں سے خوفزدہ نہ ہوں۔ یہ کتابوں میں مذکور بہت پرانا حربہ ہے۔ اگر ایجنٹ کے لئے وارنٹ یا پروانۂ طلبی حاصل کرلینا اتنا ہی آسان ہوتا تو، اس نے آپ کا رضاکارانہ تعاون حاصل کرنے کی کوشش میں وقت صرف نہ کیا ہوتا۔ ایک بار پھر یاد دلادیں کہ، کہ آپ بس یہ کہدیں کہ آپ کسی تلاشی کی منظوری نہیں دیتے ہیں اور یہ کہ آپ وکیل کی موجودگی کے بغیر بات نہیں کریں گے۔

## اگر کوئی ایجنٹ تلاشی کا وارنٹ موجود ھونے کا دعوی کرتا ھے تو کیا ھوگا؟

اگر کوئی ایجنٹ اپنے پاس وارنٹ موجود ہونے کا دعوی کرتا ہے تو اسے دکھانے کو کہیں۔ یہ تلاشی کے اس وارنٹ کے نمونے کی طرح نظر آنا چاہیے جیسا یہاں بیان کیا گیا ہےاور اس کے جواز کے لئے اس پر جج کا دستخط اور تاریخ درج ہونی چاہیے۔ تلاشی کا وارنٹ اس جگہ اور چیز (چیزوں) کے لئے مخصوص ہونا چاہیے جس کی تلاشی لینی ہے۔ ایجنٹ کو کسی ایسی جگوں کی تلاشی لینے کی اجازت نہ دیں جو تلاشی کے وارنٹ میں خصوصی طور پر شامل نہیں ہے۔ کسی ایجنٹ کے پاس محض تلاشی کا وارنٹ ہونے کا مطلب یہ نہیں ہوتا ہے کہ آپ کو کسی بھی سوال کا جواب دینا ضروری ہے۔ تلاشی کے دوران خاموش رہنے کا اپنا حق بنائے رکھیں – اگر آپ سے کسی سوال کا جواب دینے کو کہا جاتا ہے تو اپنا یہ عندیہ صاف صاف بتا دیں۔

## ایجنٹ کو میرے کار کی تلاشی لینے سے باز رکھنے کے لئے مجھے کیا حقوق حاصل ھیں؟

نفاذ قانون سے متعلق اہلکار کے پاس وارنٹ کے بغیر ہی کاروں کی تلاشیاں لینے کے کافی وسیع اختیارات ہوتے ہیں۔ اگر کسی ایجنٹ کے پاس یہ یقین کرنے کی امکانی وجہ ہے کہ کار میں جرم کا ثبوت موجود ہے تو، ایجنٹ، وارنٹ کے بغیر، گاڑی کی اور گاڑی کے اندر رکھے کسی بھی ایسے ڈبے کی تلاشی لے سکتا / سکتی ہے جو اس قدر بڑا ہو جس میں وہ آئٹم آسکتا ہو جس کی تلاش کے لئے اس کے پاس امکانی وجہ موجود ہے۔ مثلا، اگر کسی ایجنٹ کے پاس یہ یقین کرنے کی امکانی وجہ موجود ہے کہ آپ نے بڑا سا ٹیلیویژن چرایا ہے تو وہ کار کے ٹرنک کی تلاشی لے سکتا ہے لیکن دستانے والے خانے یا ٹرنک میں رکھے اوزار والے ڈبے کی تلاشی نہیں لے سکتا / سکتی ہے۔ اگر اس کے پاس کار کے اندر حال ہی میں رکھے گئے ڈبے کی تلاشی لینے کی امکانی وجہ موجود ہے تو، وہ صرف اسی ڈبے کی تلاشی لے سکتا / سکتی ہے۔ اگر آپ گرفتار کیے جاتے ہیں اور آپ کی کار تحویل میں لے لی جاتی ہے تو، نفاذ قانون سے متعلق اہلکار کو وارنٹ کے بغیر فہرست مشمولات کی تلاشی لینے کی اجازت ہے۔ بنیادی طور پر اس کا مطلب یہ ہے کہ کار کے اندر جو کچھ بھی موجود ہے اس کی فہرست سازی کے مقصد سے وہ آپ کی کار کی تلاشی لے سکتا / سکتی ہے، لیکن وہ وہاں پر پائی جانے والی کوئی بھی چیز کسی بھی وجہ سے آپ کے خلاف استعمال کرسکتا / کرسکتی ہے۔ فرد سامان کی تلاشی مقامی طور پر طے شدہ طریق کار کے مطابق ہونی چاہیے،اور پولیس فرد سامان کی تلاشی کو وارنٹ کے بغیر تلاشی لینے کے لئے امکانی وجہ کے بطور استعمال نہیں کرسکتی ہے۔

## اگر میرے دفتر یا گھر میں توڑ پھوڑ ہوئی ہے اور مجھے شبہ ہے کہ اس کا محرک خفیہ معلومات اکٹھا کرنا تھا تو مجھے کیا کرنا چاہیے؟

اگرآپ کے گھر یا آفس کو توڑا گیا ہے، یا آپ ، آپ کی تنظیم یا آپ جس فرد کے ساتھ کام کرتے ہیں اس کے خلاف دھمکیاں دی گئی ہیں تو، اس سے متاثر ہونے والے ہر فرد کے ساتھ اس معلومات کا اشتراک کریں اور ذاتی و دفتر کے تحفظ میں اضافہ کے فوری اقدامات کریں۔ فوری طور پر کسی وکیل سے رابطہ کریں۔

## "درپردہ اور چوری چھپے" تلاشیاں

"درپردہ اور چوری چھپے" تلاشیوں سے حکومت کو، عدالت سے خفیہ منظوری لے کر، تلاش کیے جانے والے متعلقہ فرد کو مطلع کیے بغیر تلاشیاں لینے اور اس پر نگاہ رکھنے کی اجازت مل جاتی ہے۔ چونکہ درپردہ اور چوری چھپے تلاشیاں خفیہ طور پر انجام دینے کا ارادہ ہوتا ہے، لہذا وہ عام طور پر توڑ پھوڑ کر کے اندر گھس کر انجام دی جاتی ہیں۔

عام طور پر ایجنٹ کو پہلے جج کے سامنے حاضر ہونا اور تلاشی کا وارنٹ حاصل کرنے کے واسطے امکانی وجہ بیان کرنا ہوتا ہے۔ تاہم، فارن انٹلیجنس سرویلینس کورٹ میں ایجنٹ درپردہ اور چوری چھپے تلاشی لینے کے لئے اجازت حاصل کرسکتے ہیں اگر وہ یہ ثابت کرسکیں کہ اس تلاشی سے غیر ملکی خفیہ معلومات حاصل ہوں گے۔ اور، غیر ملکی خفیہ معلومات کی جمع آوری کا تلاشی کی بنیادی وجہ ہونا ضروری نہیں ہے؛ اس کا تلاشی کی ایک زبردست وجہ ہونا کافی ہوتا ہے۔ اس کا مطلب یہ ہے کہ ایجنٹ مجرمانہ کارروائی کا ثبوت اکٹھا کرنے کے لئے آپ کے گھر کی تلاشی لینے کی اجازت حاصل کرسکتا ہے تاوقتیکہ غیر ملکی خفیہ معلومات اکٹھا کرنا بھی اس تلاشی کا ایک ہدف ہو۔

یوں تو درپردہ اور چوری چھپے تلاشی کا عمل غیر ملکی خفیہ معلومات اکٹھا کرنے کے لئے بنایا گیا تھا، مگر بیشتر عدالتوں نے درپردہ اور چوری چھپے ہونے والی تلاشیوں سے حاصل شدہ ثبوت اور معلومات کو مجرمانہ مواخذوں میں استعمال کرنے کی اجازت دے رکھی ہے۔

### ⚠ ان کے وسائل کو جانیں

## اگر ایجنٹ مجھے گرفتاری کے وارنٹ دکھاتے ہیں تو مجھے کیا کرنا چاہیے؟

اگر ایجنٹ مجھے گرفتاری کے وارنٹ دکھاتے ہیں تو مجھے کیا کرنا چاہیے؟

گرفتاری کا وارنٹ ایک وسیلہ ہے جسے پولیس اور نفاذ قانون سے متعلق اہلکار کوئی گرفتاری عمل میں لانے کے لئے آپ کے گھر میں داخل ہونے کے لئے استعمال کرتے ہیں۔ تلاشی کے وارنٹ کے تقاضوں کے بہت سارے پیچوں میں سے ایک پیچ یہ ہے کہ آپ کے گھر میں ایجنٹوں کے ایک بار داخل ہوجانے کے بعد، خواہ ان کے پاس صرف گرفتاری کا ہی وارنٹ ہو، ان کو تلاشی لینے کی زبردست آزادی مل جاتی ہے۔ وہ تلاشی کے وارنٹ کے بغیر ہی آپ کے آس پاس کی جگہ کی تلاشی لے سکتے ہیں۔ حتی کہ نفاذ قانون سے متعلق ایجنٹس "حفاظتی صفائی" کے حصے کے طور پر پورے گھر کی تلاشی لے سکتے ہیں اگر ان کے پاس یہ یقین کرنے کی معقول وجہ ہو کہ وہاں پر ایک خطرناک فرد موجود ہوسکتا ہے۔

اگر نفاذ قانون سے متعلق اہلکار گرفتاری کا وارنٹ لے کر آپ کے گھر (یا کسی اور مقام پر) پہنچتے ہیں تو، بہترین طریقہ یہ ہے کہ باہر نکل جائیں اور خود کو روپوش کرلیں۔ جاتے ہوئے دوروازہ بند کرلیں، اگر ایسا کرنا ممکن ہو۔ اگر نفاذ قانون سے متعلق ایجنٹوں کے پاس گرفتاری کا وارنٹ ہے تو، وہ آپ کو گرفتار کریں گے۔ انہیں وارنٹ کے بغیر اپنے گھر کی تلاشی لینے کی بھی مہلت نہ دیں۔

## گرفتاری کا وارنٹ

گرفتاری کا وارنٹ ایک عدالتی فرمان ہوتا ہے جو نفاذ قانون سے متعلق اہلکار کو کسی فرد خاص کو گرفتار کرنے کا اختیار دیتا ہے۔ گرفتاری کے وارنٹ پر ایک جج کا دستخط اور تاریخ درج کیا ہوا ہوتا ہے جو نفاذ قانون سے متعلق اہلکار کے ذریعہ اس امر کی تصدیق کرتے ہوئے ایک حلفیہ درخواست پر مبنی ہوتی ہے کہ کسی جرم کا ارتکاب ہونے اور وارنٹ میں نامزد فرد یا افراد کے اس جرم کے ارتکاب میں شامل ہونے کی امکانی وجہ موجود ہے۔

عمومی طور پر، پولیس اور نفاذ قانون سے متعلق ایجنٹوں کو کسی گرفتاری کے لئے وارنٹ کی ضرورت نہیں ہوتی ہے۔ اگر ان کے پاس کسی جرم کا ارتکاب ہونے کی امکانی وجہ موجود ہے تو، وہ گرفتاری عمل میں لاسکتے ہیں۔ اس اصول میں دو عمومی استثناء ہے۔ پہلا، سبھی تو نہیں مگر زیادہ تر ریاستوں میں نفاذ قانون سے متعلق ایجنٹوں کو ایسی بدعملی کے لئے گرفتاری عمل میں لانے کے لئے وارنٹ درکار ہوتا ہے جسے انہوں نے بذات خود نہیں دیکھا ہو۔ تاہم یہ ذہن نشین رکھنا ضروری ہے کہ ایجنٹ گرفتاری کے وارنٹ کے بغیر بھی ایسے سنگین جرائم کے لئے گرفتاریاں کرسکتے ہیں جسے انہوں نے نہیں دیکھا ہو۔ دوسرا، نفاذ قانون سے متعلق اہلکار کو عموما آپ کے گھر میں گرفتاری عمل میں لانے کے لئے وارنٹ درکار ہوتا ہے۔ تاہم، وہ وارنٹ کے بغیر بھی آپ کے گھر میں گرفتاری عمل میں لاسکتے ہیں اگر انہیں اس بات کا خدشہ لاحق ہونے کا یقین ہو کہ آپ ثبوت ضائع کردیں گے یا اگر وہ مسلسل کوشش کے تحت آپ کا تعاقب کر رہے ہیں اور آپ اپنے ہی یا کسی اور کے گھر میں گھس جاتے ہیں۔

### ان کے وسائل کو جانیں

## اگر مجھے پروانہ طلبی موصول ہوتا ہے تو مجھے کیا کرنا چاہیے؟

اگر مجھے پروانۂ طلبی موصول ہوتا ہے تو مجھے کیا کرنا چاہیے؟

آپ کو بذات خود پروانۂ طلبی پر مذکور عمل آوری کی تاریخ سے قبل اسے کالعدم قرار دینے کی کوشش کرنی چاہیے، لیکن اس کے باوجود بھی ایسے پروانۂ طلبی جن میں یہ مذکور ہو کہ وہ فوری تعمیل کے متقاضی ہیں وہ بھی جج کے بغیر روبہ عمل نہیں لائے جاسکتے ہیں۔

اگر کوئی فرد آپ کے دروازے پر نمودار ہوتا ہے اور آپ کو پروانۂ طلبی پیش کرتا ہے تو، بس اسے لے لیں۔ اس فرد کو اندر نہ آنے دیں، کسی سوال کا جواب نہ دیں اور تلاشی لینے کی منظوری نہ دیں۔ پروانۂ طلبی کسی ایجنٹ کو کوئی فوری کارروائی کرنے کا حق عطا نہیں کرتا ہے۔

آپ کو چاہیے کہ پروانۂ طلبی کالعدم قرار دینے میں اپنی مدد کے لئے کسی وکیل کی خدمات حاصل کریں۔ آپ کو اس بابت مطلع کیے جانے کا امکان نہ ہونے کی صورت میں کہ آپ کے بارے میں ریکارڈوں کے لئے تیسرے فریق کو پروانۂ طلبی جاری کیا گیا ہے، آپ اس پروانۂ طلبی کو کالعدم قرار دینے کی سمت پیشقدمی کرسکتے ہیں – اگر پروانۂ طلبی براہ راست آپ کو جاری نہیں کیا گیا تھا تو بھی اس سے کوئی فرق نہیں پڑتا ہے۔

# پروانہ طلبی

پروانۂ طلبی سرکاری حکام کا جاری کردہ فرمان ہوتا ہے جو کسی فرد سے اس بات کا مطالبہ کرتا ہے کہ وہ طبعی ثبوت، جیسے دستاویزات پیش کرے، یا وہ فرد عدالت میں گواہی دے۔

پروانۂ طلبی حاصل کرنا انتہائی آسان ہے۔ وہ بیشتر اوقات کسی سرکاری ملازم، عدالت کے منشی اور یہاں تک کہ نجی وکیلوں کے ذریعہ دائر کیے جاتے ہیں۔ پروانہ طلبی جاری کیے جانے سے قبل اسے جج کے سامنے پیش کرنا ضروری نہیں ہوتا ہے۔ پروانۂ طلبی جاری کرنے کے لئے درکار وجہ انتہائی معمولی ہوتی ہے؛ اگر اس امر کا کوئی معقول امکان ہے کہ مطلوبہ طبعی ثبوت یا گواہی سے چھان بین کے دائرے میں آنے والے معمول سے متعلقہ معلومات حاصل ہوجائے گی تو پروانۂ طلبی جاری کیا جاسکتا ہے۔

پروانۂ طلبی جس سہولت کے ساتھ جاری ہوجاتے ہیں وہ انہیں طاقتور وسیلہ بناتے ہیں، لیکن تلاشی کے وارنٹ اوردیگر سرکاری وسائل کے برخلاف، ان پر عمل درآمد سے قبل انہیں عدالت میں چیلنج کیا جاسکتا ہے۔ اگر آپ کو پروانۂ طلبی موصول ہوتا ہے تو، آپ پروانۂ طلبی کو "کالعدم " قرار دینے کی سمت پیشقدمی کرسکتے ہیں بشرطیکہ یہ کافی وسیع ہو یا کافی زیادہ زیربار کرنے والا ہو یا اگر یہ قانونی طور پر تحفظ یافتہ مواد، بشمول پہلی ترمیم کے ذریعہ تحفظ یافتہ مواد کا طالب ہو۔ پروانۂ طلبی ایک بار خارج ہوجانے کے بعد، اس کے وصول کنندہ سے مطلوبہ دستاویزات یا گواہی حاصل کرنے کی مزید ضرورت نہیں رہ جاتی ہے۔

پروانۂ طلبی خاص طورپر اس وجہ سے مضرت رساں ہوتے ہیں کہ نفاذ قانون سے متعلق اہلکار ان تیسرے فریقوں کو پروانۂ طلبی جاری کرسکتے ہیں جن کے پاس آپ کے بارے میں معلومات ہوسکتی ہیں۔ حکومت آپ کے ارسال کردہ ای میل کے لئے دیگر افراد کو پروانہ طلبی جاری کرسکتی ہے۔ چونکہ ان تیسرے فریقوں کو پروانۂ طلبی کالعدم قرار دینے میں ویسی دلچسپی نہیں ہوتی ہے جیس دلچسپی آپ کی ہوتی ہے، اور اس بات کا زیادہ امکان ہوتا ہے کہ وہ لڑائی جھگڑے کے بغیر پروانۂ طلبی کی تعمیل کریں گے۔

## ان کے وسائل کو جانیں

# دخل اندازی اور انسانی نگرانی

نفاذ قانون سے متعلق جدید ترین ایجنسیوں کے ذریعہ چھان بین کے عمل میں خفیہ ایجنٹوں اور مخبروں کا استعمال کرنا ناگزیر ہے۔ ترقی پسند تحریکوں یاتنظیموں میں خفیہ ایجنٹوں یا مخبروں کو بحال کرنے کی اہلیت نفاذ قانون سے متعلق اہلکار کو ایک قسم کی رسائی فراہم کرتی ہے جسے بصورت دیگر حاصل کرنا تقریبا ناممکن ہے۔ نجی افراد کی سرگرمیوں کے تعلق سے خفیہ معلومات اکٹھا کرنے کے لئے دخل اندازی کافی مفید ہے اور نفاذ قانون سے متعلق اہلکار کو چھان بین کی شروعات کرنے کے لئے کافی معلومات حاصل ہوجاتی ہے۔ خفیہ ایجنٹ اور مخبر نفاذ قانون سے متعلق اہلکار کو تحریکوں کے شرکاء، ان کی چالبازیوں اور اقدامات کےبارے میں رپورٹ پیش کرسکتے ہیں۔ یہاں تک کہ وہ شرکاء کو گرفتار کرنے کی اپنی کوششوں کے تحت غیر قانونی سرگرمی کی تجویز پیش کرسکتے، ترغیب دے سکتے اور / یا اس میں شرکت کرسکتے ہیں۔ عدالتوں نے عام طور پر یہ نتیجہ اخذ کیا ہے کہ عوامی پالیسی مخبروں کےناموں کے افشاء کو ممنوع قرار دیتی ہے سوائے اس صورت کے جب فوجداری عدالت میں دفاع کے لئے لازمی ہوجائے، لہذا مخبروں کو گواہی دینے کے لئے شاذ و نادر ہی طلب کیا جاتا ہے، جو انہیں ایک محدود نوعیت کی ذمہ داری اور جوابدہی کے ساتھ عمل کرنے کا مجاز بناتا ہے۔

## مخبر

مخبر وہ افراد ہوتے ہیں جو نفاذ قانون سے متعلق ایسے ایجنٹوں کے بطور بحال کردہ نہیں ہوتے ہیں جو نفاذ قانون سے متعلق اہلکار کو، بیشتر اوقات رقم کے بدلے، معلومات فراہم کرتے ہیں۔ مخبر معمولی طور پر اس تحریک یا تنظیم میں جس کی چھان بین یہ ایجنٹ کیا کرتے ہیں پہلے شامل رہا ہوتاہے – اور اس بارے میں اس کو کافی گھری جانکاری ہوتی ہے۔

### ان کے وسائل کو جانیں

## خفیہ ایجنٹ

خفیہ ایجنٹ نفاذ قانون سے متعلق افسر ہوتا ہے جو معلومات یا ثبوت اکٹھا کرنے کے لئے کسی تحریک یا تنظیم میں گھسنے کے لئے کوئی فرضی نام یا جعلی شناخت نامہ استعمال کرتا ہے۔
سیاسی دخل اندازی کے معاملات میں، ایجنٹ کسی مخصوص تنظیم کے لئے ایک ہمدرد کی حیثیت سے تمثیلی وضع اختیار کرے گا، اس کے کلیدی ممبروں کا اعتماد حاصل کرے گا اور پھر اس رسائی کا استعمال کرتے ہوئے خفیہ معلومات حاصل کرکے اسے چھان بین کرنے والی ایجنسیوں کے گوش گزار کرے گا۔ ایک الگ چھان بین کرنے کے لئے زمینی سطح کا کام انجام دینا ایک ثانوی مقصد ہوسکتا ہے۔ خفیہ ایجنٹ خاص طور پر مفوضہ کام کی تفصیلات کے تقاضوں کے مطابق سر ورق کی کہانی نیز ماضی اور حال کی سرگرمیوں پر محیط ایک بنیادی سوانحی اور لائق اعتبار کہانی تیار کرتے ہیں۔

### ⚠ ان کے وسائل کو جانیں

## معاون گواہ

معاون گواہ مخبروں کی طرح ہی ہوتے ہیں، سوائے اس کے کہ معاون گواہ مواخذہ کا خوف دلائے جانے کےبعد عام طور پر "دریدہ دہن" یا "مخبر" بن جانے پر رضامند ہوجاتے ہیں۔ اگر معاون گواہ کے خلاف حتمی طور پر کوئی الزام عائد کیا گیا ہے تو وہ آخرکار اپنے خلاف عائد الزامات کو کم کرنے کے بدلے میں عدالت میں گواہی دیں گے۔

نفاذ قانون سے متعلق اہلکار ایسے طبقہ کے لوگوں کو مخبر اور معاون گواہ کے طور پر بحال کرتے ہیں جو نشانہ بنائی جانے والی تحریکوں یا تنظیموں کے اندر پہلے سے فعال رہے ہوتے ہیں۔ حکومت اکثر ان افراد پر ایسے الزامات طے کرتی ہے جس سے ان کا زیادہ تر وقت جیل میں گزرے گا، پھر اس تحریک میں شامل دیگر افراد کے بارے میں مطلع کرنے کے وعدے کے بدلے میں ان کے خلاف الزامات عائد نہ کرنے کی پیشکش کرتی ہے۔ دوسری طرف، خفیہ ایجنٹ کسی بھی تحریک یا تنظیم کے ساتھ اپنی وابستگی کی ابتداء سے ہی جھوٹے بہانے استعمال کرتے ہیں۔

### ⚠ ان کے وسائل کو جانیں

## خفیہ ایجنٹ اور مخبر جو کام انجام دے سکتے ہیں کیا ان کی کوئی تحدید ہے؟

خفیہ ایجنٹ اور مخبر جو کام انجام دے سکتے ہیں کیا ان کی کوئی تحدید ہے؟

نفاذ قانون سے متعلق اہلکار کے ذریعہ خفیہ ایجنٹوں یا مخبروں کا استعمال کرنے کے تعلق سے کوئی مخصوص قانون یا تحدیدات نہیں ہیں، اور اس ضمن میں بھی کوئی بندش نہیں ہے کہ کس قسم کے جرائم کی چھان بین کے لئے دخل اندازی کا استعمال ہوسکتا ہے۔ دیگر ممالک کے برخلاف، خفیہ طریق کار استعمال کرنے کے لئے وارنٹ کی ضرورت نہیں ہوتی ہے، لہذا نفاذ قانون سے متعلق افسران کو یہ ثابت نہیں کرنا ہوتا ہے کہ اس مخصوص چھان بین کے لئے خفیہ ایجنٹ یا مخبر کا استعمال کرنا لازمی ہے۔ FBI کے ذریعہ خفیہ ایجنٹوں اور مخبروں کا استعمال خفیہ سرگرمیوں کے سلسلے میں حکومت کی کارروائی کا مطالعہ کرنے کے لئے منتخبہ کمیٹی کی حتمی رپورٹ (1976) میں مذکور یو ایس کانگریشنل کے نتائج کے بعد تشکیل شدہ ڈھیلے ڈھالے داخلی رہنما خطوط کے دائرہ کار میں آتا ہے۔

اس رپورٹ میں FBI کے اب بدنام زمانہ کاؤنٹر انٹلیجنس پروگرام (COINTELPRO) نامی پروگرام کے بارے میں تفصیلات مذکور ہیں، جو 1956 اور 1971 کے مابین رو بہ عمل تھا، جس میں فعالیت پسندوں اور تنظیموں کو نشانہ بنایا گیا تھا، اور اس میں ڈاکٹر مارٹن لوتھر کنگ، جونیئر اور بلیک پینتھر پارٹی شامل تھی۔ اس رپورٹ کے جواب میں، امریکی اٹارنی جنرل نے FBI کے خفیہ اعمال کے لئے داخلی رہنما خطوط نافذ العمل کیا جس سے خفیہ ایجنٹ اور مخبر دونوں کو ہی جواز مل گیا۔ یوں تو یہ رہنما حطوط شروع میں کافی ٹھوس تھے، مگر متعدد انتظامیہ کے ذریعہ انہیں بتدریج کمزور بنا دیا گیا ہے۔ حالیہ رہنما خطوط نفاذ قانون سے متعلق اہلکار کے بہت سارے جارحانہ طرز عمل کو جائز قرار دیتے ہیں حالانکہ اصلا تو یہ ان کا سدباب کرنے کے لئے بنائے گئے تھے۔ علاوہ ازیں، یہ رہنما خطوط عدالتوں میں رو بہ عمل لائے جانے کے قابل نہیں ہیں، لہذا وہ دخل اندازی اور نگرانی کے مقابلے میں صرف ایک محدود تحفظ ہی فراہم کرتے ہیں۔ دوسرے لفظوں میں، اگر کوئی ایجنٹ FBI کے ضوابط کی خلاف ورزی کرتے ہوئے ثبوت اکٹھا کرلیتا ہے تو بھی وہ ثبوت عدالت میں استعمال کیا جاسکتا ہے۔

## جال میں پھانسنا کیا ہے؟

خفیہ ایجنٹوں اور مخبروں کے اوپر عائد سب سے مستحکم بندش اس بات کا تقاضہ ہے کہ جال میں نہ پھانسا جائے۔ جال میں پھانسنے کا عمل اس وقت پیش آتا ہے جب کوئی ایجنٹ یا مخبر ایک ایسے فرد کے ذہن میں کسی جرم کے ارتکاب کا تصور پروان چڑھاتا ہے جو بصورت دیگر اس طرح کے جرم کے ارتکاب پر رضامند نہیں ہوتا اور پھر اس فرد کو ماخوذ قرار دینے کے لئے اسے اس جرم کا ارتکاب کرنے کی ترغیب دیتا ہے۔ عدالتیں اس دام ترغیب کو کافی ڈھیلے ڈھالے انداز میں لیتی ہیں، اور غیر قانونی سرگرمی کی تجویز کرنے یا ترغیب دینے والے خفیہ ایجنٹوں یا مخبروں کو بڑی آزادی عنایت کرتی ہیں۔ یوں تو دام ترغیب کے دفاع کے سلسلے میں استثناء ریاست در ریاست الگ الگ ہے، لیکن اگر خفیہ ایجنٹ نے محض اس جرم کے ارتکاب کی تجویز کی ہے تو عام طور پر یہ کوئی مؤثر دفاع نہیں ہوتا ہے۔ بہت ساری ریاستوں میں اگر جیوری کو اس امر کا یقین ہے کہ کوئی فرد جرم کا ارتکاب کرنے پر پہلے سے ہی اس پر آمادہ تھا تو دام ترغیب کوئی بدیہی مدافعت نہیں ہوتی ہے ۔ دوسری ریاستوں میں، دام ترغیب صرف اسی صورت میں مدافعت ہوتی ہے جب وہ جرم "جسمانی مضرت کا باعث یا دھمکی" پر مشتمل ہو۔ انہی وجوہات کے پیش نظر، کوئی فرد دام ترغیب کے دفاع کی دستیابی پر انحصار نہیں کرسکتا ہے۔

## دخل اندازی کرنے کے کسی ایجنٹ کے اختیار پر کون سی دستوری تحدیدات لاحق ہیں؟

خفیہ ایجنٹوں اور مخبروں کو عموما عوامی میٹنگوں میں، نیز عبادت گاہوں میں ہونے والی اجتماعات میں جانے کی اجازت ہوتی ہے۔ عدالتوں کو کبھی کبھار یہ تعین ہونے پر کہ نفاذ قانون سے متعلق ایجنٹوں نے تقریر اور وابستگی کی آزادی کے حقوق بروئے کار لانے کی کسی جماعت کی اہلیت میں مداخلت کی ہے پہلی ترمیم کی خلاف ورزی ہونے کا علم ہوا ہے۔ اسی طرح، عدالتوں نے نفاذ قانون سے متعلق اہلکار کو کسی فعالیت پسند یا تنظیم سے متعلق معلومات اکٹھا کرکے اسے عوامی طور پر جاری کرنے کے معاملے میں پہلی ترمیم کی خلاف ورزی میں ملوث پایا ہے۔ عدالتوں کو ایسی صورت میں پہلی ترمیم کی خلاف ورزی ہونے کا کوئی علم نہیں ہے جب نفاذ قانون سے متعلق ایجنٹ عوامی میٹنگوں میں محض ایک تکلیف دہ ماحول پیدا کرتے ہیں۔

عدالتیں معمول کے مطابق اس نتیجے پر پہنچی ہیں کہ خفیہ ایجنٹوں اور مخبروں کے ذریعہ ہونے والی بات چیت کی خفیہ ریکارڈنگ سے چوتھی ترمیم کی خلاف ورزی نہیں ہوتی ہے، جو کہ غیر مناسب تلاشی اور ضبطیوں کے خلاف تحفظ فراہم کرتی ہے۔

عدالتیں اس نتیجے پر بھی پہنچی ہیں کہ خفیہ ایجنٹوں اور مخبروں کے ذریعہ ہونے والی بات چیت کی خفیہ ریکارڈنگ سے خود کو ملزم قرار دینے کے خلاف پانچویں ترمیم کے تحفظ کی خلاف ورزی نہیں ہوتی ہے۔ اسی طرح اگر آپ انجانے طور پر کسی خفیہ ایجنٹ یا مخبر کو اپنے گھر میں یا کسی دیگر نجی جگہ پر بلاتے ہیں تو، عدالتیں اس چیز کو اس ایجنٹ کے ذریعہ تلاشی لینے کی "منظوری" مانتی ہیں۔ اگر خفیہ ایجنٹ کو جرم کی ممکنہ وجہ نظر آتی ہے تو، وہ نفاذ قانون سے متعلق دیگر ایجنٹوں کو خفیہ ایجنٹ کو حاصل شدہ اس مبینہ منظوری کی بنیاد پر تلاشی کے عمل میں شامل ہونے کے لئے بلاسکتا / سکتی ہے۔ کچھ عدالتوں نے ایسے حالات کے لئے بھی وہی منطقی استدلال لاگو کر رکھا ہے جن حالات میں انجانے طور پر کسی مخبر کو کسی گھر میں داخل ہونے کے لئے بلانے کا نشانہ بنایا جاتا ہے۔

## میں دخل اندازی کے ثبوت کا تعین کس طرح کرسکتا ہوں؟

دخل اندازی کرنے والے کی نشاندہی کے لئے کچھ مفید اشارے موجود ہیں۔ خفیہ ایجنٹ یا مخبر ایسے کام انجام دینے کے لئے رضاکارانہ طور پر تیار ہوسکتا ہے جن سے آپ کی جماعت کی اہم میٹنگوں اور کاغذات تک رسائی فراہم ہوتی ہیں، جیسے مالی ریکارڈز، اراکین کی فہرست، روداد اور خفیہ فائلیں۔ خفیہ ایجنٹ اور مخبر بیشتر اوقات تشدد یا غیر قانونی حربے استعمال کرنے کی ترغیب دیتے یا استدلال پیش کرتے ہیں اور ان حربوں کی مخالفت کرنے والے دیگر افراد پر ڈرپوک ہونے کا الزام عائد کرتے ہیں۔ اسی طرح، خفیہ ایجنٹ اور مخبر اکثر دوسروں کے اوپر خفیہ ایجنٹ اور مخبر ہونے کا الزام عائد کرتے ہیں، اس طرح وہ اپنی ذات کے اوپر سے توجہ ہٹادیتے ہیں اور پھر اپنے کام سے جماعت کی توجہ منتشر کردیتے ہیں۔ خفیہ ایجنٹ یا مخبر کے پاس ایک لمبے عرصے تک آمدنی کا کوئی ظاہری وسیلہ نہیں ہوتا ہے یا ان کے کام سے انہیں جتنی تنخواہ ملنی چاہیے اس سے زیادہ رقم ان کے پاس دستیاب ہوتی ہے۔

مشکوک ایجنٹ یا مخبر کے پس منظر کے بارے میں معلومات حاصل کرنے کی کوشش کریں۔ وہ مشکوک ایجنٹ ماضی میں جن علاقوں میں رہا / رہی ہے وہاں کی تنظیموں سے معلوم کریں تاکہ یہ پتہ چل جائے کہ آیا کوئی فرد اس کی ضمانت دے سکتا ہے۔ پتہ کریں کہ آپ انٹرنیٹ پر کون سا نتیجہ برآمد برآمد کرسکتے ہے۔ عوامی ریکارڈز جیسے کریڈٹ رپورٹ، ووٹر رجسٹریشن اور رہن ناموں میں کافی معلومات ہوتی ہے، نیز ماضی اور حال کا پتہ بھی موجود ہوتا ہے۔ اگر وہ دستیاب ہیں تو، آپ کو مقامی پولیس اکیڈمی کے سند یافتگان کی فہرست میں تلاش کرنا چاہیے؛ لیکن، یاد رکھیں کہ ہوسکتا ہے کہ وہ مشکوک فرد اپنا اصلی نام استعمال نہیں کر رہا ہو۔

خصوصیات کی اس درجہ بندی پر صادق آنے والا فرد لازمی طور پر خفیہ ایجنٹ یا مخبر نہیں ہوتا ہے۔ احتیاط بروئے کار لائیں اور کسی فرد پر خفیہ ایجنٹ یا مخبر ہونے کا الزام اس وقت تک نہ لگائیں جب تک آپ کے پاس اس کے خلاف ٹھوس ثبوت موجود نہ ہو۔

## میں اپنی تنظیم کو بچانے کے لئے کون سی احتیاطی تدابیر کرسکتا ہوں؟

نگرانی اور مداخلت کے سبھی مشکوک یا مصدقہ تجربات کی فائل سنبھال کر رکھیں۔ اس میں تاریخ؛ مقام؛ وقت؛ حاضرین؛ وہاں پیش آنے والی ہر چیز کی پوری وضاحت؛ اور اس تجربے کی سیاق و سباق کی وضاحت کرنے والا کوئی تبصرہ اور اس وقوعہ کی وجہ سے فرد یا تنظیم پر پڑنے والے اثرات کی وضاحت شامل کریں۔ سراغ رسانی اور ایذا رسانی پر گفتگو کرنے کے لئے ایک میٹنگ کریں، اور تعین کریں کہ آیا آپ کے کسی ممبر کو ایذا رسانی کا سامنا ہوا ہے یا نگرانی والی کوئی ایسی سرگرمی ان کے علم میں آئی ہے جس کے ذریعہ اس تنظیم کی سرگرمیوں کو نشانہ بنایا گیا ہو۔ اپنی جماعت میں ماضی کی مشکوک سرگرمیوں یا مشکلات کا تجزیہ کریں، اور یہ تعین کرنے کی کوشش کریں کہ آیا ایک یا زیادہ افراد ان میں سے بہت سارے واقعات میں شامل رہے ہیں۔

آپ ایجنسیوں جیسے FBI، ڈپارٹمنٹ آف ہوم لینڈ سیکیورٹی (DHS)، بیورو آف الکحل، ٹوبیکو اینڈ فائر آرمس اور دیگر وفاقی ایجنسیوں کے پاس اپنی تنظیم کے لئے فریڈم آف انفارمیشن ایکٹ (FOIA) کی عرضیاں دائر کرنے کی کوشش کرسکتے ہیں۔ قوانین اطلاعات کے سلسلے میں اپنی ریاست کی آزادی کو بروئے کار لاتے ہوئے نفاذ قانون سے متعلق مقامی اور ریاستی ایجنسیوں کے پاس اسی طرح کی عرضیاں دائر کریں۔ سب سے اہم بات، اپنی تحریک یا تنظیم کو مفلوج بنا دینے والی دخل اندازی کے بارے میں مخبوط الحواس نہ ہوں۔ مخبوط الحواسی بھی بذات خود دخل اندازی کی طرح ہی تخریب کن ہوسکتی ہے۔

# الیکٹرانک نگرانی

اس باب میں ان طریقوں کو بیان کیا گیا ہے جنہیں ایجنٹ اپنی چھان بین میں استعمال کرسکتے ہیں یعنی ٹیلیفون وائر ٹیپ، بگ اور انٹرنیٹ نگرانی۔ چونکہ ہماری زندگیاں پہلے سے کہیں زیادہ ڈیجیٹل ہوگئی ہیں، لہذا ایجنٹ بھی معلومات اکٹھا کرنے کے لئے روز افزوں طور پر الیکٹرانک نگرانی کا استعمال کر رہے ہیں۔ بدقسمتی سے، قانون اور عدالتیں عام طور پر ٹکنالوجی کی رفتار کے ساتھ چلنے میں ناکام رہ جاتی ہیں، جو اکثر و بیشتر تازہ ترین ٹکنالوجی کے پیش نظر نامعلوم یا لا یعنی رازداری کے تحفظ کا پیش خیمہ ہوتا ہے۔

استقلال پذیری کا ایک اچھا اصول ہے: مواصلت کے ذرائع جتنے ہی پرانے ہوتے ہیں، قانون اسے اتنا ہی زیادہ تحفظ عطا کرتا ہے۔ ایلیٹ اسپٹزر (Elliot Spitzer) جب نیو یارک ریاست کے اٹارنی جنرل تھے تو انہوں نے کہا تھا، "اگر آپ بات کرسکتے ہیں تو تحریر کا سہارا نہ لیں۔ جب آپ سر ہلاکر کام چلا سکتے ہوں تو بات ہرگز نہ کریں۔ اور ای میل میں تو کبھی کوئی چیز نہ رکھیں کیونکہ یہ تو موت کے مترادف ہے۔ آپ ہمیں درکار سارا ثبوت استغاثہ کو فراہم کر رہے ہوتے ہیں۔"

# ٹیلیفون مواصلات

ٹیلیفون پر ہونے والی بات چیت میں کئی ایک طریقوں – ٹیپ، بگز، متحرک وائر ٹیپ، پین رجسٹر سے لے کر جال میں پھانسنے اور تعاقب کرنے والے آلات تک – سے رکاوٹ پیدا کی جاسکتی ہے۔ ٹیلیفون نگرانی کے طریقے تفصیلی اور کافی پیچیدہ ہیں اور ہم یہاں پر صرف ان کا مجموعی جائزہ ہی پیش کرسکتے ہیں۔ تاہم، یہ سبق آسان سا ہے – ٹیلیفون پر آپ جو کچھ بھی کہتے ہیں اس بارے میں کافی محتاط رہیں۔

حکومت کو عام طور پر آپ کا فون ٹیپ کرنے کے لئے ٹائٹل III وائرٹیپ آرڈر کے نام سے موسوم ایک خصوصی وارنٹ درکار ہوتا ہے۔ تاہم، حکومت فوری موت یا سنگین چوٹ، قومی سلامتی یا منظم جرائم کی خصوصیات رکھنے والی سرگرمیوں پر مشتمل مخصوص ہنگامی حالات کے تحت 48 گھنٹے تک بغیر وارنٹ کے بھی آپ کا فون ٹیپ کرسکتی ہے۔ حکومت بعد میں نگرانی جاری رکھنے کی اجازت حاصل کرنے کے لئے وارنٹ طلب کرسکتی ہے جس میں اس سے پہلے والی وائر ٹیپنگ شامل ہوتی ہے۔

## حکومت میری فون کالیں کب ٹیپ کرسکتی ہے؟

# ٹائٹل III وائر ٹیپ آرڈرز

ٹائٹل III وائر ٹیپ آرڈرز ایسے وارنٹ ہوتے ہیں جو آپ کی مواصلت میں رکاوٹ ڈالنے اور اس پر نگاہ رکھنے کے لئے استعمال ہوتے ہیں۔ زیادہ تر تلاشیوں کے لئے تلاشی کے وارنٹ کا مطالبہ کرنے والی چوتھی ترمیم کی تحفظات کے علاوہ، کانگریس نے اومنیبس کرائم کنٹرول اینڈ سیف اسٹریٹس ایکٹ [Omnibus Crime Control and Safe Streets Act - 1968] کے ٹائٹل III میں زبانی مواصلت کے ضمن میں اضافی تحفظات فراہم کیے۔ یہ اضافی تحفظات 1960 کی دہائی میں FBI کے ذریعہ وسیع پیمانے پر پھیلی ہوئی غیر قانونی اور ناگوار نگرانی کے کانگریشنل نتائج کے جواب میں پاس ہوئے تھے (ملاحظہ کریں 'خفیہ ایجنٹ اور مخبر جو کام انجام دے سکتے ہیں کیا ان کی کوئی تحدید ہے؟")۔

ایجنٹوں کو ٹائٹل III کی ایک طویل درخواست پیش کرنی چاہیے جس میں شامل ہو: جس جرم کا ارتکاب ہوا ہے یا ارتکاب ہونے والا ہے اس بارے میں حقائق؛ وہ مقام جہاں سے اس مواصلت میں رکاوٹ پیدا کی جائے گی؛ وہ مواصلات جن میں رکاوٹ پیدا کی جاتی ہے؛ آیا چھان بین کے دیگر حربے بروئے کار لائے گئے ہیں اور وہ ناموزوں ثابت ہوئے تھے یا یہ کہ دیگر حربے لاگو کرنا ناموزوں یا کافی زیادہ مضرت رساں ہوگا؛ جو رکاوٹ ڈالی جاتی ہے اس کے لئے پیمانہ وقت؛ اور اس طرح کے ہدف یا احاطوں کے تعلق سے وائرٹیپ کی سبھی سابقہ درخواستوں پر مذکور بیان۔

ٹائٹل III وائر ٹیپ آرڈر جاری کرنے کے لئے، جج کو پتہ لگانا چاہیے: اس امر کی امکانی وجہ کہ نشانہ بنایا جانے والا وہ فرد ٹائٹل III کے دائرے میں آنے والے جرم کا ارتکاب کر رہا ہے؛ کہ اس جرم سے تعلق رکھنے والی مواصلت اس میں رکاوٹ پیدا کرکے ہی حاصل کی جاسکتی ہے؛ اور یہ کہ جن سہولیات کی مدد سے مواصلت میں رکاوٹ پیدا کی جائے گی انہیں جرم کے سلسلے میں استعمال کیا جا رہا ہے۔

اصل کے اعتبار سے ٹائٹل III سے صرف سنگین جرائم کے ایک محدود زمرے کے نگرانی کی اجازت ملی۔ گزرتے سالوں میں، کانگریس نے زیادہ سے زیادہ جرائم کو ٹائٹل III کے دائرے میں شامل کردیا ہے۔ آج، قانون سیکڑوں جرائم پر محیط ہے، جس میں منشیات، بلوہ، فحاشی، یا تجارت میں خلل ڈالنے پر مشتمل جرائم جیسے وسیع زمرے بھی شامل ہیں۔ان جرائم کی ایسے وسیع مطالب سے فعالیت پسندی کی بہت ساری شکلوں کی نگرانی کرنے کی اجازت مل جاتی ہے۔

## ان کے وسائل کو جانیں

## ٹائٹل III وائرٹیپ آرڈرز (جاری)

ٹائٹل III وائرٹیپ آرڈرز ابتدائی طور پر 30 دنوں تک برقرار رہ سکتے ہیں۔ نفاذ قانون سے متعلق اہلکار دوبارہ سے 30 دنوں کی توسیع کے لئے جج سے رجوع کرسکتے ہیں۔ ٹائٹل III وائرٹیپ آرڈر کا دورانیہ ختم ہوجانے کے بعد، جج وائر ٹیپ کا نشانہ بنائے جانے والوں کی مواصلات میں رکاوٹ پیدا کرنے کی فہرست کو بند کرنے کا فرمان جاری کرسکتا ہے۔ اس طرح کی فہرست سے وائر ٹیپ کے مقررہ عرصے میں نشانہ بنائے جانے والے فرد کی اور اس امر کی اطلاع ملتی ہے کہ آیا مواصلت میں واقعی رکاوٹ پیدا کی گئی تھی۔ تاہم، اس کے بعد بھی جج یہ انتخاب کرسکتا ہے کہ اس طرح کی فہرست جاری کرنے کا مطالبہ نہ کیا جائے۔

عام طور پر، نفاذ قانون سے متعلق اہلکار کے لئے وائر ٹیپ کے فرامین حاصل کرنے کا عمل شاذ و نادر ہی پیش آتا ہے؛ لیکن جب بھی وہ اسے حاصل کرنا چاہتے ہیں لگ بھگ ہمیشہ ہی انہیں یہ فرمان حاصل ہوجاتا ہے۔ مثلاً، 2007 میں، وائر ٹیپ کے فرامین کے لئے ریاستی اور وفاقی عدالتوں میں صرف 2,208 درخواستیں جمع کروائی گئی تھی، لیکن اس سال ساری ہی درخواست منظور ہوگئی تھیں۔ وائرٹیپ کے فرامین کی سب سے زیادہ تعداد آبکاری کے معاملات میں (2,208 میں سے 1,792 یا 81 فیصد) تھی، جبکہ اس کے بعد سب سے زیادہ تعداد قتل عمد اور دست درازی کے معاملات کی (2,208 میں سے 132 یا 6 فیصد) تھی۔

## ⚠ ان کے وسائل کو جانیں

### اگر میرا فون ٹیپ ہو رہا ہے تو مجھے کیسے معلوم ہوگا؟

زیادہ امکان تو یہی ہے کہ اگر آپ کا فون ٹیپ ہو رہا ہے تو آپ کو معلوم ہی نہیں ہوگا۔ حکومت کی نگرانی کے سلسلے میں اس وقت کے بعد سے زبردست پیشرفت ہوئی ہے جب سے کلک، بیپ، بز کی آوازیں اور کسی اور آواز سے آپ کو ٹیپ کیے جانے کا اشارہ مل سکتا تھا۔ عام طور پر یہ فرض کیا جاتا ہے کہ حکومت نگرانی ختم ہونے کے بعد 90 دنوں کے اندر آپ کو بتا دے گی لیکن، متعلقہ سہولت کے پیش نظر اس اطلاع نامہ کو ملتوی بھی کیا جاسکتا ہے۔

### متحرک وائرٹیپ کیا ہے؟

تمثیلی طور پر، وائرٹیپ کو عدالتی فرمان کے ذریعہ جواز مل جانے پر اس کا اطلاق مخصوص مقام پر مخصوص فون پر ہوتا ہے۔ تاہم، متحرک وائر ٹیپ کسی بھی فون پر کسی بھی ایسے مقام پر کیا جانے والا ٹیپ ہے جس جگہ کے بارے میں نفاذ قانون سے متعلق اہلکار کو یقین ہو کہ ہدف بنایا جانے والا فرد فون کالیں کرے گا۔ متحرک وائرٹیپ کو 1998 سے ہی سرکاری استعمال کے لئے اجازت ملی ہوئی ہے۔ حکومت کو متحرک وائر ٹیپ کے لئے بھی انہی معیارات کی تکمیل کرنی ہوتی ہے جن معیارات کی تکمیل مستقل ٹیپ کے لئے کرنی ہوتی ہے – یعنی اس امر کی امکانی وجہ کہ جرم کا ارتکاب ہوا ہے یا ہونے والا ہے۔

## بگز کے بارے میں کیا خیال ہے؟

بگ ایک انتہائی چھوٹا الیکٹرانک آلہ ہوتا ہے جس سے کوئی گفتگو سنی کی جاسکتی، نشر کی جاسکتی اور / یا ریکارڈ کی جاسکتی ہے۔ آپ کے گھر یا دفتر میں بگ رکھ کر نفاذ قانون سے متعلق اہلکار اس آلے کے دائرے میں رہتے ہوئے ہونے والی ایک ایک بات کو سن سکتا ہے۔ بگ کے استعمال پر نافذ العمل تقاضے عموما وہی ہیں جو وائرٹیپ کے لئے ہیں۔ بگ کے استعمال سے نفاذ قانون سے متعلق ایجنٹوں کو کچھ خلقی پریشانیاں لاحق ہوتی ہیں: ان کا ابدافی جگہ میں نصب ہونا ضروری ہوتا ہے؛ ان میں چھیڑ چھاڑ کیے جانے کا امکان رہتا ہے؛ اس کے پتہ لگ جانے کا خطرہ رہتا ہے؛ اور الیکٹریکل انداز کی مداخلتیں کر کے اسے بیکار کیا جاسکتا ہے۔ ان پریشانیوں کی وجہ سے وائر ٹیپ کے مقابلے بگ کا استعمال ہونے کا امکان کافی کم ہوتا ہے۔

## پین رجسٹرز اور "جال میں پھانسنے اور تعاقب کرنے" والے آلات

پین رجسٹر آلہ اس ٹیلیفون لائن سے ڈائل کیے جانے والے نمبروں کو ریکارڈ کرتا ہے جس لائن کے ساتھ وہ آلہ منسلک کیا ہوتا ہے۔ "جال میں پھانسنے اور تعاقب کرنے" والے آلات آنے والی ٹیلیفون کالوں کے نمبر بھی ریکارڈ کرتے ہیں۔

اگر نفاذ قانون سے متعلق اہلکار اس میں سے کوئی بھی آلہ نصب کرنا اور استعمال کرنا چاہتا ہے تو اس کے لئے عدالتی فرمان ضروری ہوتا ہے؛ تاہم، یہ عدالتی فرامین حاصل کرنا کافی آسان ہے۔ حکومت کو صرف اس امر کا یقین کرنا ہوتا ہے کہ جو معلومات حاصل ہونے کا امکان ہے اس کا تعلق رواں مجرمانہ چھان بین سے ہے۔ جج صاحبان اور نفاذ قانون سے متعلق اہلکار خاص طور پر کسی چھان بین سے جس چیز کا تعلق ہونے کا امکان ہوتا ہے اس پر کافی کشادہ نظریہ اپناتے ہیں۔ بہت ساری ریاستیں کافی غیر محتاط معیارات کے تحت بھی اس طرح کی نگرانی کی اجازت دیتی ہیں۔ نیز امریکی اٹارنی جنرل بھی مخصوص۔

پین رجسٹر آلہ اس ٹیلیفون لائن سے ڈائل کیے جانے والے نمبروں کو ریکارڈ کرتا ہے جس لائن کے ساتھ وہ آلہ منسلک کیا ہوتا ہے۔ "جال میں پھانسنے اور تعاقب کرنے" والے آلات آنے والی ٹیلیفون کالوں کے نمبر بھی ریکارڈ کرتے ہیں۔

### ان کے وسائل کو جانیں

## پین رجسٹرز اور
## "جال میں پھانسنے اور تعاقب کرنے" والے آلات (جاری)

اگر نفاذ قانون سے متعلق اہلکار اس میں سے کوئی بھی آلہ نصب کرنا اور استعمال کرنا چاہتا ہے تو اس کے لئے عدالتی فرمان ضروری ہوتا ہے؛ تاہم، یہ عدالتی فرامین حاصل کرنا کافی آسان ہے۔ حکومت کو صرف اس امر کا یقین کرنا ہوتا ہے کہ جو معلومات حاصل ہونے کا امکان ہے اس کا تعلق رواں مجرمانہ چھان بین سے ہے۔ جج صاحبان اور نفاذ قانون سے متعلق اہلکار خاص طور پر کسی چھان بین سے جس چیز کا تعلق ہونے کا امکان ہوتا ہے اس پر کافی کشادہ نظریہ اپناتے ہیں۔ بہت ساری ریاستیں کافی غیر محتاط معیارات کے تحت بھی اس طرح کی نگرانی کی اجازت دیتی ہیں۔ نیز امریکی اٹارنی جنرل بھی مخصوص۔

## ان کے وسائل کو جانیں

## فارن انٹیلیجنس سرویلینس کورٹ اور نیشنل سیکیورٹی ایجنسی کی بلا وارنٹ وائر ٹیپنگ پروگرام کے بارے میں کیا خیال ہے؟

اگر یہ یقین کرنے کی امکانی وجہ موجو د ہو کہ نشانہ بنایا جانے والا فرد کسی غیر ملکی دہشت گرد گروپ کا رکن یا کسی غیر ملکی طاقت کا ایجنٹ ہے تو حکومت شہری اور غیر ملکی دونوں کی ہی وائرٹیپنگ کرسکتی ہے۔ شہریوں اور از روئے قانون مستقل مکینوں کی وائرٹیپنگ کے واسطے، حکومت کو اس امر کی امکانی وجہ بھی پیش کرنی چاہیے کہ نشانہ بنایا جانے والا فرد ایسی سرگرمیوں میں ملوث ہے جس میں مجرمانہ خلاف ورزی شامل "ہوسکتی" ہے۔ اس قسم کی نگرانی کے لئے، فارن انٹیلیجنس سرویلنس کورٹ سے تلاشی کا وارنٹ حاصل کرنا چاہیے، یہ ایک خفیہ عدالت ہوتی ہے جس میں ہونے والی سماعتیں اور ریکارڈز عوام کے لئے بند ہوتے ہیں۔ حکومت نیشنل سیکیورٹی ایجنسی (NSA) کے توسط سے، بغیر وارنٹ کے کسی ٹیلیفون یا الیکٹرانک مواصلت پر نگاہ رکھنے کے اختیار کا دعوی کرتی ہے اگر اسے اس امر کا یقین ہو کہ ایک فریق امریکہ سے باہر ہے - خواہ دوسرا فریق امریکہ میں ہی ہو۔ ویسے تو NSA کو صرف غیر ملکی خفیہ معلومات حاصل کرنے کے مقصد کے پیش نظر مواصلات پر نگاہ رکھنے کا اختیار ہے، مگر اس پروگرام کی پوری حد معلوم نہیں ہے۔

## سیلولر فونز، اسمارٹ فون اور PDAs میں سیکیورٹی کے کون سے خدشات لاحق ہوتے ہیں؟

سیل فون پر ہونے والی مواصلات کی سہولت اور آسانی کے ساتھ رازداری اور سلامتی کے اہم خطرات بھی جڑے ہوتے ہیں۔ ان آلات کے استعمال میں شامل خلقی خطرات سے آگاہ رہیں اور ہر بار سیل فون استعمال کرنے سے قبل سلامتی کے خطرے کے پیش نظر سہولت والے فائدے کا اندازہ لگائیں۔

سیل فون پر بھی ٹیپنگ، پین رجسٹر یا جال میں

## سیلولر فونز، اسمارٹ فون اور PDAs میں سیکیورٹی کے کون سے خدشات لاحق ہوتے ہیں؟ (جاری...)

پھانسنے اور تعاقب کرنے والے آلات حاصل کرنے کے وہی قانونی اصول لاگو ہوتے ہیں جو اصول لینڈ لائنوں پر لاگو ہوتے ہیں۔ تاہم، یہ ذہن نشیں رکھنا ضروری ہے کہ چند سو ڈالرز کی قیمت والے آلات سے لیس کوئی بھی فرد آپ کے سیل فون کے سگنلز میں رکاوٹ پیدا کرسکتا ہے۔ اور، آپ کو یہ نہیں مان لینا چاہیے کہ ایجنٹ ہمیشہ قانون کی پیروی کرتے ہیں۔ افراد اور کارپوریشنز بھی آسانی سے آپ کے سیل فون کے سگنلز میں رکاوٹ پیدا کرسکتے ہیں نیز پکڑے جانے کا خطرہ کم ہی ہوگا۔

حکومت کے پاس یہ صلاحیت ہے کہ کسی سیل فون کو صرف سننے والے آلے یا "متحرک بگ" میں تبدیل کردے۔ اس سے حکومت کو آپ کے سیل فون کے قریب ہونے والی کوئی بھی بات چیت سننے کی سہولت حاصل ہوجاتی ہے۔ حکومت کو متحرک بگ "لگانے" کے لئے سیل فون تک رسائی درکار نہیں ہوتی ہے، بلکہ وہ محض آپ کے سیل فون کمپنی کی معرفت ہی اس کا آغاز کرسکتی ہے۔ حکومت کو متحرک بگ سے آپ کے سیل فون کے قریب ہونے والی گفتگو سننے کی سہولت حاصل ہوجاتی ہے خواہ آپ کے سیل فون کا سوئچ آف ہو۔ تاہم، ایسا لگتا ہے کہ سیل فون سے بیٹری کو طبعی طور پر نکال دینے پر متحرک بگ غیر فعال ہوجائے گا۔

آپ کا سیل فون آپ کے جائے وقوع کا پتہ لگانے کے لئے بھی استعمال ہوسکتا ہے۔ جب بھی آپ کا سیل فون چالو ہوتا ہے اور اس کا سگنل مل جاتا ہے، اس کا ربط آپ کے علاقے میں موجود ایک سے زیادہ سیل ٹاور سے ہوجاتا ہے۔ حکومت آپ کا طبعی جائے وقوع متعین کرنے کے لئے ان رابطوں پر نگاہ رکھ سکتی ہے۔ شہروں اور ان دیگر علاقوں میں جہاں سیلولر ٹاورز کافی زیادہ تعداد میں ہوتے ہیں، آپ کا جائے وقوع زیادہ قطعیت کے ساتھ، کبھی کبھار تو چند گز کے اندر ہی پتہ چل سکتا ہے۔ فی الحال سیل فون کے اس قسم کے تعاقب کے لئے کوئی یکساں قانونی معیار نہیں ہے۔ کچھ عدالتیں تو ایجنٹوں سے پین رجسٹر یا جال میں پھانسنے اور تعاقب کرنے والے آلات حاصل کرنے کے لئے درکار ویسی ہی قانونی شہادت کا مطالبہ کرتی ہیں جبکہ دیگر عدالتیں ایجنٹوں سے ایک وارنٹ بھی حاصل کرنے کا مطالبہ کرتی ہیں جس کی تائید میں امکانی وجہ بھی موجود ہو۔ حکومت اس وقت آپ کے جائے وقوع کا تعین کرنے کے لئے آپ کے سابقہ سیل فون کے ریکارڈز بھی دیکھ سکتی ہے اگر اس وقت آپ کا سیل فون آف رہا تھا۔

کچھ عدالتوں نے یہ فیصلہ صادر کیا ہے کہ آپ کے گرفتار ہونے کے بعد، نفاذ قانون سے متعلق اہلکار، وارنٹ لے کر، کال کی روداد اور آپ کے سیل فون میں ذخیرہ کردہ رابطوں کو تلاش کرسکتے ہیں۔ کچھ عدالتوں نے یہ فیصلہ بھی صادر کیا ہے کہ قانونی گرفتاری کے بعد، نفاذ قانون سے متعلق اہلکار متنی پیغامات، تصاویر، ای میل اور آپ کے فون میں موجود کوئی اور ریکارڈ بھی تلاش کرسکتے ہیں۔ کچھ عدالتیں نفاذ قانون سے متعلق اہلکاروں کو وارنٹ کے بغیر کال کی سرگزشت، اس دلیل کے ساتھ تلاش کرنے کی اجازت دیتی ہیں کہ کال کی سرگزشت سے اسی معلومات کا خلاصہ ہوگا جو پین رجسٹر سے حاصل ہوسکتا ہے، لیکن متنی پیغامات یا ای میل کی تلاشی لینے کے لئے وارنٹ کی ضرورت ہوتی ہے۔ عدالتیں ابھی بھی قانون کے اس شعبے کو فروغ دے رہی ہیں؛ نتیجے کے طور پر، قوانین اور ضوابط ایک عدالتی دائرہ اختیار سے دوسرے عدالتی دائرہ اختیار تک الگ الگ ہوسکتے ہیں۔ اپنے سیل فون پر پاسورڈ والے تحفظات کو فعال کردینے سے سیل فون کے استعمال کے ساتھ خلقی طور پر لاحق سلامتی کے خطرات کے خلاف کچھ حد تک تحفظ حاصل ہوجاتا ہے۔

## کیا حکومت میرے متنی پیغامات (ٹیکسٹ میسیجز) پر نگاہ رکھ سکتی ہے؟

متنی پیغام کو مواصلت کا غیر محفوظ طریقہ مانا جاتا ہے ۔ سیل فون پر ہونے والی مواصلت کی طرح، متنی پیغامات میں کسی بھی فرد کے ذریعہ اچھی قسم کے آلے کی مدد سے بہ آسانی رکاوٹ ڈالی جاسکتی ہے۔ کانگریس اور عدالتیں دونوں میں کسی کو بھی اس بارے میں واضح طور پر معلوم نہیں ہے کہ آیا متنی پیغامات میں رکاوٹ ڈالنے کے لئے امکانی وجہ اور وارنٹ کی موجودگی ضروری ہے، لہذا نفاذ قانون سے متعلق اہلکار پین رجسٹر یا جال میں پھانسنے اور تعاقب کرنے کے ایسے فرامین استعمال کرکے جنہیں حاصل کرنا نسبتا آسان ہے متنی پیغامات میں رکاوٹ ڈال سکتے ہیں۔ آخری بات، چونکہ متنی پیغامات کو "تار" والی مواصلت نہیں مانا جاتا ہے، لہذا انہیں وائرٹیپ ایکٹ کے استثنائی اصول کے ذریعہ تحفظ حاصل نہیں ہے۔ لہذا اگرچہ حکومت غیر قانونی طریقے سے آپ کے متنی پیغامات میں رکاوٹ پیدا کرتی ہے، مگر اس کے باوجود بھی وہ ان مواصلات کو آپ کے خلاف مجرمانہ مقدمے میں استعمال کرسکتی ہے۔

# انٹرنیٹ مواصلات

## کیا حکومت میرے ای میل پڑھ سکتی؟

نفاذ قانون سے متعلق اہلکار آپ کے زیادہ تر الیکٹرانک مواصلات اور اس میں مذکور معلومات تک بہ آسانی رسائی حاصل کرسکتے ہیں۔ آپ کے الیکٹرانک مواصلات تک رسائی کے لئے پروانۂ طلبی حاصل کرنے کی خاطر، حکومت کو صرف یہ ثابت کرنا ہوتا ہے کہ جو معلومات حاصل ہونے کا امکان ہے اس کا تعلق مجرمانہ معاملے کی جاری چھان بین سے ہے۔ پروانۂ طلبی حاصل کرکے، حکومت آپ کی "استعمال کنندہ کی بنیادی معلومات" حاصل کرسکتی ہے، جس میں اکاؤنٹ کے ساتھ وابستہ نام اور رہائشی پتہ؛ زیر استعمال خدمات کی طوالت اور نوعیت، سیشن لاگز، اور آپ کے کمپیوٹر کا IP ایڈریس شامل ہوتا ہے۔

حکومت کو بغیر مواد والے دیگر ریکارڈز حاصل کرنے کے لئے ایک D آرڈر (ملاحظہ کریں "ان کے وسائل کو جانیں: D آرڈرز:") درکار ہوتا ہے، جس میں کوئی بھی ایسا ریکارڈ یا لاگ شامل ہوتا ہے جس سے وہ ای میل پتہ جس پر آپ ای میل بھیجتے ہیں یا جس سے آپ کو ای میل موصول ہوتا ہے؛ وقت اور تاریخیں جب ای میل بھیجے یا وصول کئے گئے تھے؛ اور ہر ای میل کی جسامت کا پتہ چلتا ہے۔

تیسرے فریق جیسے ویب ای میل سروس، یا انٹرنیٹ سروس پرووائڈر (ISP) کے ذریعہ ذخیرہ کردہ ای میل کے سلسلے میں، مختلف تحفظات لاگو ہوتے ہیں جن کا انحصار اس امر پر ہوتا ہے کہ کوئی ای میل کس حد تک جدید ترین ہے اور یا آپ نے اسے پڑھا ہے یا نہیں۔ ذخیرہ کردہ وواصلات سے متعلق ایکٹ (Stored Commu-nications Act) نفاذ قانون سے متعلق اہلکار سے تقاضہ کرتا ہے کہ 80 دنوں سے کم عرصہ سے ذخیرے میں رکھے ہوئے بند پڑے ای میلز کے مواد (موضوع والی سطر اور نفس مضمون) کے لئے تلاشی کا وارنٹ حاصل کریں۔ 80 دن سے زیادہ عرصہ سے بند پڑے ای میلز اور تیسرے فریق کے ذریعہ ذخیرے میں رکھے ہوئے بند پڑے ای میلز کے لئے، حکومت کو ای میل کے مواد کے لئے ایک D آرڈر حاصل کرنا چاہیے یا پروانۂ طلبی جاری کرنا چاہیے۔ حکومت 180 دن سے زیادہ پرانے یا کھلے ہوئے ای میلز کے لئے تلاشی کا وارنٹ حاصل کرنے کا بھی انتخاب کرسکتی ہے۔

الاسکا، اریزونا، کیلیفورنیا، ہوائی، ایڈاہو، مونٹانا، نیویڈا، اوریگن اور واشنگٹن میں، جو نائنتھ سرکٹ کورٹ آف اپیلز (Ninth Circuit Court of Appeals) کے دائرے میں آنے والی ریاستیں ہیں، عدالتوں نے حکومت کی اس مطلب بیانی سے اختلاف رائے کیا ہے کہ، وہ D آرڈر کے ساتھ، 180 دنوں سے کم عرصہ سے ذخیرے میں موجود کھلے ہوئے ای میلز حاصل کرسکتی ہے۔ ان عدالتوں نے یہ فرمان جاری کیا ہے کہ حکومت کو 180 دن سے کم عرصہ والے کسی بھی ای میل کے لئے وارنٹ درکار ہوتا ہے۔

یہ فرض کیا جاتا ہے کہ حکومت ای میل کا مواد حاصل کرنے کے لئے D آرڈرز یا پروانۂ طلبی استعمال کرنے سے قبل انفرادی صارف کو اس کی اطلاع کردے۔ اصولی طور پر اس کی وجہ سے صارف کو پروانۂ طلبی پر تیسرے فریق کے عمل درآمد کرنے سے پہلے ہی اسے آگے بڑھانے یا کالعدم قرار دینے کی سہولت مل جائے گی۔ تاہم، ذخیرہ کردہ مواصلات سے متعلق ایکٹ کا ایک اور ضابطہ نفاذ قانون سے متعلق اہلکار کو D آرڈرز یا پروانۂ طلبی کی اطلاع کوایک مخصوص مقررہ عرصہ تک کے لئے مؤخر۔

## کیا حکومت میرے ای میل پڑھ سکتی؟ (جاری...)

کردینے کا اختیار عطا کرتا ہے، اور ایسا لگتا ہے کہ حکومت مستقل طور پر اطلاعات کو مؤخر کرتی ہے۔ نفاذ قانون سے متعلق اہلکار تلاشی کا وارنٹ کے لئے درکار اضافی اقدامات اختیار کرکے آپ کو کوئی نوٹس دینے سے احتراز بھی کرسکتے ہیں۔

بڑے بڑے ISPs کو ان کے صارفین کے بارے میں معلومات حاصل کرنے کے لئے ہر ماہ 1,000 سے زیادہ پروانۂ طلبی موصول ہوتے ہیں۔ بیشتر پروانۂ طلبی میں صارفین کے نام، پتے، ISP کے پتے اور اس بات کے ریکارڈز مطلوب ہوتے ہیں کہ اہدافی فرد نے انٹرنیٹ پر کب سائن آن اور سائن آف کیا۔
نفاذ قانون کے پروگراموں کی بہت ساری ایسی رپورٹیں موجود ہیں جو انٹرنیٹ کی کافی زیادہ بھیڑ بھاڑ کو قابو میں کرنے کے لئے تیار کی گئی ہیں، جن میں ای میل اور ویب سرگرمی بھی شامل ہے۔ ان پروگراموں کی گنجائش، ان کا مجاز استعمال اور ان کے توسط سے حاصل کردہ کسی معلومات کا عدالت میں وجۂ جواز فی الحال معلوم نہیں ہے۔

## کیا حکومت بتاسکتی ہے کہ میں کون سی ویب سائٹیں دیکھتا ہوں؟

نفاذ قانون سے متعلق اہلکار کو آپ کے ذریعہ دیکھی جانے والی اصل ویب سائٹوں کے ریکارڈز کے لئے وارنٹ کی ضرورت ہوتی ہے۔ حکومت مبینہ طور پر آپ کی دیکھی ہوئی ویب سائٹ کا یونیفارم ریسورس لوکیٹر (URL) ایڈریس، جیسے e.g. http://ccrjustice.org بغیر وارنٹ کے حاصل کرسکتی ہے؛ لیکن حکومت کو ویب سائٹ پر آپ کے دیکھے ہوئے مخصوص صفحات جیسے، http://ccrjustice.org/ifanagentknocks پر موجود معلومات کو حاصل کرنے کے لئے وارنٹ درکار ہوتا ہے۔

## "Dآرڈرز"

نفاذ قانون سے متعلق اہلکار کا ایک اور وسیلہ 2307(D) آرڈر ہے، جس کو عام طور پر "D آرڈر" کہا جاتا ہے۔ اس آرڈر کو یہ نام ذخیرہ کردہ مواصلات سے متعلق ایکٹ کے ذیلی حصے سے دیا گیا تھا جو انہیں اختیار عطا کرتا ہے۔ حکومت تیسرے فریقوں کے ذریعہ ذخیرہ کردہ الیکٹرانک ریکارڈز – بیشتر اوقات ای میلز، حاصل کرنے کے لئے D آرڈر کا استعمال کرتی ہے۔ سادہ پروانۂ طلبی حاصل کرنے کی بہ نسبت D آرڈرز حاصل کرنا زیادہ مشکل ہے لیکن تلاشی وارنٹ کے بہ نسبت اسے حاصل کرنا زیادہ آسان ہے۔ D آرڈر حاصل کرنے کے لئے، حکومت کو جج کے سامنے خصوصی حقائق پیش کرنے چاہئیں جس سے یہ ثابت  ہو کہ حاصل ہونے والی معلومات کا تعلق مجرمانہ معاملے کی رواں چھان بین سے ہونے کا یقین کرنے کی معقول وجوہات موجود ہیں۔ لہذا D آرڈر  کے لئے مطلوب شبہہ ممکنہ وجہ کی بہ نسبت کمتر ہے، لیکن پروانۂ طلبی حاصل کرنے کے واسطے مطلوب "کسی معقول امکان" کی بہ نسبت  اعلی تر ہے۔

**تعرف على أدواتهم**

## کیا مجھے غیر سرکاری اداروں کی جانب سے ہونے والی الیکٹرانک نگرانی کی بابت فکر مند ہونا چاہیے؟

کارپوریٹ جاسوسی شاید حکومت کی جاسوسی کی بہ نسبت کافی بڑی صنعت ہے۔ کارپوریشنز ایسے فعالیت پسندوں کی نگرانی کروانے کے لئے جو ان کے مفادات کو نقصان پہنچاسکتے ہیں، معمول کے مطابق نجی جاسوسوں کی خدمات حاصل کرتی ہیں، جن میں سے زیادہ تر تو نفاذ قانون سے متعلق سابق ایجنٹ ہوتے ہیں۔ کارپوریٹ جاسوسی میں وہی حربے شامل ہوتے ہیں جو حکومت کے ذریعہ اپنائے جاتے ہیں، بشمول: ردی کو الٹ پلٹ کر تلاشی لینا؛ ٹیلیفونز ٹیپ کرنا؛ انٹرنیٹ والی سرگرمی پر نگاہ رکھنا؛ اور دخل اندازی کا استعمال کرنا۔ قانونی بندشوں یا جاسوسی کی وجہ سے کارپوریٹ جاسوسی کے بارے میں تشویش لاحق ہونے کا امکان شاید کم ہے۔

## نیشنل سیکیورٹی لیٹرز

نیشنل سیکیورٹی لیٹر (NSL) ایک وسیلہ ہے جسے FBI کسی تیسرے فریق مثلا ٹیلیفون کمپنی، ISP، کنزیومر کریڈٹ ایجنسی یا مالیاتی ادارے سے کسی فرد کے بارے میں خفیہ طور پر معلومات حاصل کرنے کے لئے استعمال کرتی ہے۔ NSL کے لئے کسی امکانی وجہ یا سرسری جائزہ مطلوب نہیں ہوتا ہے - FBI کو صرف یہ یقین کرنا ہوتا ہے کہ انہیں حاصل ہونے والی معلومات کا تعلق دہشت گردی یا جاسوسی کی چھان بین سے ہے۔ NSL کے قانون میں زبان بندی کا ایک بنا بنایا اصول ہے جو NSL وصول کرنے والے کسی فرد کو اپنے وکیل کے علاوہ کسی اور فرد سے یہ بتانے سے ممنوع قرار دیتا ہے کہ انہیں یہ موصول ہوا ہے۔ یوں تو عدالت کے ایک حالیہ فرمان میں مستقل، زبان بندی کے بنے بنائے اصول کو غیر دستوری مانا گیا ہے، مگر آئندہ اس کے اطلاق کی بابت ابھی بھی وضاحت نہیں ہے۔

سرکاری مطالعات میں یہ بتایا گیا ہے کہ FBI ایک سال میں دسیوں ہزار NSLs جاری کرتا ہے، اور بسا اوقات یہ خطوط جاری کرنے میں ان کے اختیار پر معمولی سی بھی بندش ہونے پر وہ اس کی خلاف ورزی کربیٹھتا ہے۔ NSLs سے حاصل شدہ ڈیٹا کا اشتراک امریکی انٹلیجنس برادری، دیگر سرکاری ایجنسیوں، اوریہاں تک کہ غیر ملکی حکومتوں کے ساتھ ہوتا ہے۔ اگر آپ کو یا آپ جس تنظیم میں کام کرتے ہیں اس کو کوئی NSL موصول ہوتا ہے تو، فوری طور پر کسی وکیل سے رابطہ کریں۔

### ان کے وسائل کو جانیں

# الیکٹرانک سیکیورٹی

الیکٹرانک سیکیورٹی ایک استقرائی اور پیچیدہ عنوان ہے۔ اس حصے میں الیکٹرانک سیکیورٹی کے سلسلے میں کچھ بنیادی مشورہ متعارف کروایا گیا ہے۔ آپ کو ان سارے عنوانات پر مزید گہری معلومات اس کتابچہ کے اضافی وسائل والے حصے میں ملیں گے۔

آسان لفظوں میں، سب سے محفوظ الیکٹرانک مواصلت یہ ہے کہ الیکٹرانک مواصلت بالکل بھی نہ کی جائے۔ الیکٹرانک سیکیورٹی کی مؤثر عادات الیکٹرانک مواصلت کے ساتھ وابستہ سہولت اور خطرات کے مابین ایک دیرپا توازن برقرار رکھنے کی متقاضی ہوتی ہیں۔ جیسا کہ کسی بھی طرز عمل میں ہوتا ہے، آپ کو یہ فیصلہ کرتے وقت کہ الیکٹرانک سیکیورٹی کے کون سے اقدامات اپنائے جائیں، فوائد کو سامنے رکھ کر خطرات کی قدر پیمائی کرنی چاہیے۔

## ڈیٹا کی مرموزکاری

مرموزکاری معلومات کو ایک خفیہ کوڈ میں تبدیل کرنے کا طریقہ ہے۔ اگر مناسب طریقے سے استعمال کیا جائے تو، مرموزکاری آپ کے ڈیٹا کو کسی دیگر ایسے فرد کے ذریعہ دیکھے جانے سے تحفظ فراہم کرتی ہے جس کے پاس اسے دیکھنے کے لئے مناسب "کلید" نہیں ہے۔ مرموزکاری کی جدید ترین ٹکنالوجی اس قدر ٹھوس ہے کہ اصولی طور پر حکومت کے لئے بھی کلیدوں کا استعمال کیے بغیر مرموز پیغامات کو غیر مرموز کرنا ناممکن ہے۔ مرموزکاری حکومت کو آپ کا الیکٹرانک ڈیٹا حاصل کرنے سے محفوظ رکھنے کا سب سے مستحکم تحفظ ہے۔

وسیع پیمانے پر دستیاب پروگراموں سے آپ کو اپنے ہارڈ ڈرائیو میں سبھی ڈیٹا کو مرموز کرکے رکھنے کی سہولت حاصل ہوتی ہے۔ آپ کے کمپیوٹر پر لاگ ان کرنے کے لئے معمولی نوعیت کے پاسورڈز آپ کے ہارڈ ویئر کو تحفظ فراہم کرنے کے لئے کافی نہیں ہیں۔ حکومت ہارڈ ڈرائیو لے سکتی، اس کی ایک کاپی بناسکتی اور آپ کے لاگ ان کے بغیر ڈیٹا تک آسانی سے رسائی حاصل کرسکتی ہے۔

مرموز ہارڈ ڈرائیو کی مدد سے، آپ کی فائلوں کو کوڈ میں بدلا جاسکتا ہے اور حکومت کو آپ کے مرموز پاسورڈ کے بغیر ان تک رسائی حاصل نہیں ہوسکے گی۔

مرموزکاری کے پروگراموں سے انفرادی فائلوں یا فولڈروں کو بھی مرموز کرنے کی سہولت حاصل ہوجاتی ہے۔ یوں تو اس کا انتظام کرنا آسان ہوسکتا ہے لیکن غیر منظور شدہ مرموز کاری سے ان فائلوں کو اضافی خدشات بھی لاحق ہوسکتی ہیں۔ ایک بہتر تدبیر یہ ہے کہ حساس نوعیت کی فائلوں کے لئے ایک علاحدہ، کلی طور پر مرموز ہارڈ ڈرائیو رکھا جائے۔

## اپنے وسائل کو جانیں

# الیکٹرانک سیکیورٹی

## ای میل کی مرموزکاری

مرموزکاری کا استعمال کرنا ای میل کے لئے پہلے سے کہیں زیادہ اہم ہے۔ ہم نے پہلے ہی بتا دیا ہے کہ حکومت آپ کے ای میل تک رسائی حاصل کرنے کے لئے کس طرح D آرڈرز یا پروانۂ طلبی استعمال کرسکتی ہے یا ان کی ترسیل میں رکاوٹ ڈالنے کے لئے دیگر آلات استعمال کرسکتی ہے۔ اور، ای میل ایک بار تیسرے فریق کے کمپیوٹر پر پہنچ جانے کے بعد، آپ کو اس امر پر کوئی اختیار نہیں رہ جاتا ہے کہ کون اسے حاصل کر اور پڑھ سکتا ہے۔ ڈیٹا کی مرموزکاری کی طرح ہی، آپ کے الیکٹرانک مواصلت کو محفوظ کرنے کا ایک طریقہ ہے ای میل کو مرموز کرنا۔ تاہم، ای میل کی مرموزکاری مؤثر طریقے سے استعمال کرنے کے لئے، آپ کو بھی اور جس فرد کے ساتھ آپ مواصلت کر رہے ہیں اس کو بھی مرموزکاری کا پروگرام لازما استعمال کرنا چاہیے۔

ای میل کی مرموزکاری یہ یقینی بناتی ہے کہ صرف ارادی وصول کنندگان ہی آپ کا ارسال کردہ ای میل پڑھ سکیں۔ ای میل کی جدید ترین موموزکاری "عوامی کلید" کے نظام کی معرفت کام کرتی ہے۔ ایک عوامی کلید اس ضمن میں ہدایات، یا کوڈ فراہم کرتی ہے کہ آپ کو ارسال کردہ ای میل کیسے واضح ہوگا۔ غیر واضح پیغامات کا کوڈ – "نجی کلید" – عوامی کلید سے مختلف ہوتا ہے، اور صرف آپ کو ہی نجی کلید تک رسائی حاصل ہوتی ہے۔ اگر پروانۂ طلبی، عدالتی فرمان کے ذریعہ یا بصورت دیگر آپ کے ای میل میں رکاوٹ ڈالی گئی ہے تو،اس کے تحت موجود پیغامات کو آپ کی نجی کلید کے بغیر واضح نہیں کیا جاسکتا ہے۔

یوں تو ای میل کی مرموزکاری کے مزید تکنیکی پہلو اس قدر تفصیلی ہیں کہ انہیں اس کتابچے میں شامل نہیں کیا جاسکتا، مگر کھلا ہوا دروازہ جسے مقفل تو کوئی بھی فرد کرسکتا ہو لیکن صرف وہی فرد کھول سکتا ہو جس کے پاس مخصوص کلید ہو مرموزکاری کی ایک آسان سی یکسانیت ہے۔

ای میل کی مرموزکاری کا استعمال کرنا آج ماضی کی بہ نسبت زیادہ آسان ہے۔ GNU پرائیویسی گارڈ (GnuPG) ایک مفت پروگرام ہے جسے ای میل کے زیادہ تر بڑے پروگراموں میں ضم کیا جاسکتا ہے۔ مثال کے طور پر، تیسرے فریق کا میل کلائنٹ موزیلا تھنڈر برڈ ایک پلگ ان پیش کرتا ہے، جسے سیکیورٹی ایکسٹنشن کے نام سے جانا جاتا ہے، جس کو Enigmail کہا جاتا ہے جو GnuPG کے ساتھ مطابقت پذیر ہے اور اس کی وجہ سے مرموزکاری کو استعمال کرنا کافی آسان ہوجاتا ہے۔

### اپنے وسائل کو جانیں

# الیکٹرانک سیکیورٹی

## پاسورڈز

پاسورڈز کو سنجیدگی سے لیں۔ کوئی لفظ یا ایسا لفظ جس کے آخر میں یا بیچ میں کوئی عدد بھی ہو استعمال نہ کریں۔ وہ پاسورڈز چند کوششوں کے بعد آسانی سے توڑے جاسکتے ہیں۔ حروف کی ایک ایسی ترتیب استعمال کریں جو صرف آپ کے لئے بامعنی ہوں۔

جس اکاؤنٹ میں نجی معلومات ہوں ان کے لئے ایک ہی پاسورڈ دوبار استعمال نہ کریں۔ اپنا پاسورڈ اپنے دماغ میں محفوظ رکھنے کی کوشش کریں۔ تحریری پاسورڈز دریافت ہوسکتے ہیں یا ان کے لئے پروانۂ طلبی جاری کیا جاسکتا ہے۔ ہر دو مہینے پر اپنا پاسورڈ تبدیل کریں۔ اگر آپ اپنا پاسورڈ تحریر کرکے ہی رکھتے ہیں تو، اسے ایسے کوڈ میں تحریر کرنے کی کوشش کریں جسے صرف آپ ہی سمجھتے ہوں۔ اگر آپ پاسورڈ لکھتے ہیں تو، اسے اپنے کمپیوٹر کے بغل میں یا اس کے پاس ہرگز نہ چھوڑیں؛ اسے اپنے بٹوے سے الگ رکھنا ہی بہتر ہوتا ہے۔

"پاسورڈ سیف" ("password safe") نامی پروگرام استعمال کرنے کی کوشش کریں۔ ان پروگراموں سے آپ کو اپنے پاسورڈز اپنے کمپیوٹر پر ایک واحد مرموز فائل میں سنبھال کر رکھنے میں سہولت ملتی ہے اس طرح آپ کو اپنے دیگر سبھی پاسورڈز تک رسای کے لئے صرف ایک ہی پاسورڈ یاد رکھنا ہوتا ہے۔ اپنا ماسٹر پاسورڈ کبھی بھی تحریر کرکے نہ رکھیں، کیونکہ یہی پاسورڈ دیگر سبھی کو تحفظ عطا کرتا ہے۔

## ویب براؤزنگ

جو ڈیٹا آپ کا ویب براؤز آپ کی انٹرنیٹ سرگرمی کے ضمن میں سنبھال کر رکھ سکتا ہے اور جو ڈیٹا دیگر ویب سائٹیں آپ کے بارے میں اپنے پاس رکھ سکتی ہیں ان کا نظم و نسق احتیاط کے ساتھ کریں۔

بطور ڈیفالٹ، انٹرنیٹ براؤزرز امکانی طور پر نجی معلومات کا ایک بڑا حصہ اپنے پاس رکھتے ہیں، جس میں درج ذیل شامل ہیں لیکن یہ انہی تک محدود نہیں ہیں: جو ویب سائٹیں آپ دیکھتے ہیں؛ ان ویب سائٹوں کے پاسورڈز؛ اور یہاں تک کہ آپ نے جو ویب صفحہ دیکھا ہے اس سے اخذ کردہ تصویریں۔ جس ایجنٹ کو آپ کے ہارڈ ڈرائیو پر تسلط حاصل ہوجاتا ہے وہ ان فائلوں سے آپ کی انٹرنیٹ سرگرمیوں کے بارے میں کافی ساری معلومات حاصل کرسکتا ہے۔ یہ معلومات باقاعدگی سے حذف کرتے رہیں۔ اپنے انٹرنیٹ براؤزنگ کی سرگزشت، ذخیرہ، کوکیز، ڈاؤن لوڈ کی سرگزشت، محفوظ کردہ فارم اور محفوظ کردہ پاسورڈز باقاعدگی سے حذف کرتے رہنے کے لحاظ سے اپنا براؤزر ترتیب دیں۔

جب بھی دستیاب ہو، براؤزنگ کے وقت ویب سائٹ کی بنی بنائی مرموزکاری استعمال کریں تاکہ تیسرے فریق ترسیل کردہ معلومات میں رکاوٹ پیدا نہ کرسکیں۔ جن ویب سائٹوں میں بنی بنائی مرموزکاری ہوتی ہے ان کی شروعات میں http کے بجائے https ہوتا ہے۔ انٹرنیٹ کے گمنام ٹولز جیسے Tor استعمال کرنے کی کوشش کریں۔ Tor ایک مرموزکاری اور گمنام بنانے والا پروگرام ہے جو آپ کے ڈیٹا میں صرف Tor کے دیگر کلائنٹس کی معرفت چلتا ہے، اثنائے راہ آپ کے ڈیٹا کو مرموز کرتا ہے اور ڈیٹا جہاں سے وجود میں آیا تھا اس جگہ کے بارے میں معلومات کو ختم کردیتا ہے۔

## اپنے وسائل کو جانیں

# الیکٹرانک سیکیورٹی

## ویب براؤزنگ (جاری ...)

ہر Tor کے راؤٹر کو صرف اس آخری راؤٹر کا پتہ معلوم ہوتا ہے جہاں سے اس کا گزر ہوا تھا، جس کی وجہ سے کسی مواصلت کے اصل ماخذ پر واپس جاکر اس کا پتہ لگانا مشکل ہوجاتا ہے۔ Tor استعمال کرنے کی کچھ خامیاں یہ ہیں کہ ویب صفحات جس رفتار سے لوڈ ہوتے ہیں وہ رفتار سست ہوجاتی ہے، اور بہت سارے غیر محفوظ فنکشن جیسے فلیش Tor کے اوپر کام نہیں کرتے ہیں۔

## اپنے انٹرنیٹ خدمت فراہم کنندگان کو جانیں

آپ جس الیکٹرانک خدمت کے لئے بھی سائن اپ کرنے پر غور کر رہے ہیں اس کی خدمت کی شرائط اور رازداری کی پالیسیاں پڑھیں۔ کچھ ISPs بشمول متعدد ایسی خدمات جو سیاسی سرگرمیوں کی ضرورتوں کے لئے تیار کردہ ہیں، رازداری کی مستحکم تر تحفظات فراہم کرتی ہیں، اور حکومت کی استفسارات کے تئیں زیادہ سے زیادہ مزاحم ہونے کا دعوی کرتی ہیں۔

## اینٹی اسپائی ویئر پروگرامز استعمال کریں

اچھا اسپائی ویئر اور / یا اینٹی وائرس پروگرام خریدیں اور باقاعدگی سے اس کی تجدید کریں۔ اسپائی ویئر آپ کے سبھی الیکٹرانک سیکیورٹی کی حکم عدولی کرسکتا ہے، آپ جو بھی ویب سائٹ دیکھتے ہیں اور اپنی مشین پر آپ جو بھی کلید دباتے ہیں اس پر یہ لاگ ان ہوسکتا ہے۔ اسپائی ویئر کی بڑی بڑی کمپنیوں کا دعوی ہے کہ وہ سرکارئی اسپائی ویئر کے ساتھ بھی ویسا ہی برتاؤ کرتے ہیں جیسا برتاؤ دیگر اسپائی ویئر کے ساتھ کرتے ہیں۔

## ڈیٹا کو سنبھال کر رکھنا اور حذف کرنا

جو چیز موجود نہیں ہے اس کو حکومت حاصل نہیں کرسکتی ہے۔ ڈیٹا کو سنبھال کر رکھنے کی ایک پالیسی بنائیں اور آپ اس پالیسی کے تحت باقاعدگی سے پرانی فائلوں کا تجزیہ کرکے انہیں حذف کریں۔ چننده فائلیں ضائع نہ کریں - ایک مقررہ وقت طے کریں اور اس پر کاربند رہیں۔ آپ مختلف قسم کے ڈیٹا کے لئے مختلف نظام الاوقات طے کرسکتے ہیں، جیسے کمپیوٹر کی فائلیں ہر دو مہینے پر حذف کریں؛ ای میل ہر دو ہفتے پر حذف کریں؛ اور ویب براؤزر کے اندراجات ہر دو دن پر حذف کریں۔ پالیسی جو بھی ہو اس پر کاربند رہیں۔ بہرحال، کیا آپ کو پچھلے تین سال کے ای میلز کی واقعتا ضرورت ہے؟

کوئی ایسی چیز ضائع نہ کریں جس کے لئے پروانۂ طلبی جاری کیا گیا ہے – اگر آپ ایسا کرتے ہیں تو، الزام کی شفافیت میں چھیڑ چھاڑ کرنے کے سنگین خطرے میں مبتلا ہوجائیں گے۔ ثبوت کو ضائع کرنے کے الزامات سے اپنی ذات کو اور اپنی تنظیم کو محفوظ رکھنے کے لئے ڈیٹا سنبھال کر رکھنے کی اپنی پالیسی کا ایک تحریری ریکارڈ رکھیں۔

## اپنے وسائل کو جانیں

# گرانڈ جیوری اور گرانڈ جیوری کی مزاحمت

گرانڈ جیوری شہریوں کا ایک پینل ہوتا ہے جو جرائم کی چھان بین کرنے اور قرار داد جرم جاری کرنے کے لئے تشکیل دیا ہوتا ہے۔ اپنے اصل تصور کے لحاظ سے، گرانڈ جیوری کا مقصد تھا انتہاپسندانہ لحاظ سے جمہوریت پسند ہونا۔ انگلینڈ میں، انھوں نے شہریوں اور شہنشاہ اور ان کے استغاثہ کے مابین بفر کی حیثیت سے خدمات انجام دیں۔ امریکہ کے ابتدائی ایام میں، کوئی بھی شہری اصل گرانڈ جیوری پر بدعملی کا الزام عائد کرسکتا تھا اور گرانڈ جیوری کو اکثریتی ووٹ سے بے دخل کیا جاسکتا تھا۔

جدید دور کی گرانڈ جیوری کافی مختلف ہیں۔ آج، سبھی مقدمات استغاثہ کے ذریعہ گرانڈ جیوری کے سامنے پیش کیے جاتے ہیں۔ استغاثہ گواہ کو بلاتا ہے اور سوالات پوچھتا ہے۔ گواہوں کو وکیل پیش کرنے کی اجازت نہیں ہوتی ہے۔ اس میں جج حاضر نہیں ہوتا ہے۔ استغاثہ الزامات کا مسودہ تیار کرتا ہے اور انہیں گرانڈ جیوری کے سامنے پڑھتا ہے۔ اس میں یہ مطالبہ نہیں ہوتا ہے کہ

گرانڈ جیوری کے ممبران کو اس معاملے پر قانون کے تعلق سے ہدایت دی جائے۔ اور، دیگر جیوریز کے برخلاف، تعصب کے پیش نظر گرانڈ جیوری کے ممبران کی اسکریننگ نہیں ہوتی ہے۔

چونکہ استغاثہ ہی کلی طور پر قانونی کارروائیاں ترتیب دیتا ہے، لہذا اس بات پر کوئی حیرت نہیں ہونی چاہیے کہ گرانڈ جیوری لگ بھگ ہمیشہ ہی استغاثہ کے لئے ایک ربر اسٹامپ کی طرح کام کرتی ہے۔ نیو یارک کے ایک سابق چیف جج نے ایک بار نمایاں طور پر تحریر کیا کہ "کوئی استغاثہ اگر ایک مضر سینڈوچ کو ملزم قرار دینا چاہے تو وہ اسے بھی ملزم قرار دے سکتا ہے۔" شاذ و نادر طور پر جب گرانڈ جیوری ملزم قرار نہیں دیتی ہے، استغاثہ مختلف گرانڈ جیوری کا ایک پینل تیار کرتا ہے اور نئی گرانڈ جیوری کے سامنے فرد قرار دار جرم کا مطالبہ کرتا ہے۔

**گرانڈ جیوری کیا ہیں اور فعالیت پسندوں کے لئے وہ کس قسم کے خطرات کے حامل ہوتے ہیں؟**

سیاسی معاملات میں، گرانڈ جیوریز کا استعمال فعالیت پسندوں کے خلاف الزام تراشیوں کو انجام تک پہنچانے کے لئے استعمال ہوا ہے۔ استغاثہ کسی فعالیت پسند گواہ کو لائیں گے اور انہیں کسی اور فعالیت پسند کی مخبری کرنے پر مجبور کرنے کی کوشش کریں گے

## گرانڈ جیوری کیا ھیں اور فعالیت پسندوں کے لئے وہ کس قسم کے خطرات کے حامل ھوتے ھیں؟ (جاری...)

نیز اگر وہ گرانڈ جیوری کے ساتھ تعاون کرنے سے انکار کریں تو جیل میں ڈالنے کی دھمکی دیتے ہیں۔ یہ جان لینا ضروری ہے کہ گرانڈ جیوری کس طریقے سے کام کرتی ہے؛ آپ کے کیا حقوق ہیں؛ آپ کن حقوق پر عمل درآمد نہیں کرسکتے ہیں؛ اور گرانڈ جیوری کی کیسے مخالفت کی جائے۔

ہمیں حاصل شدہ بہت سارے حقوق گرانڈ جیوری کے گواہوں کے لئے کوئی وجود نہیں رکھتے ہیں۔ گرانڈ جیوری کے گواہ کو یہ حق نہیں ہے کہ وکیل کے ذریعہ اس کی نمائندگی کی جائے اور اگر انہیں جیل میں ڈالنے کی دھمکی دی جاتی ہےتو انہیں جیوری کی سماعت کا حق نہیں ہے۔ گرانڈ جیوری کے گواہ کو خود کو ملزم قرار دیئے جانے کے خلاف حق ضرور حاصل ہے لیکن اس کے باوجود بھی اسے خود کو اور دوسروں کو مواخذہ اور سزا سے مامون رکھنے کے بدلے میں مخبری کرنے پر مجبور کیا جاسکتاہے۔ مامونیت صرف گواہوں کو تحفظ فراہم کرتی ہے--دوسرے افراد کا اس کے بعد بھی مواخذہ ہوسکتا ہے۔

## اگر کوئی فرد گرانڈ جیوری کا پروانہ طلبی دکھاتا ہے تو مجھے کیا کرنا چاہیے؟

گرانڈ جیوری کے پروانۂ طلبی نفاذ قانون سے متعلق ایجنٹوں، خاص طور پر پولیس افسران اور وفاقی مارشلوں کے ذریعہ پیش کیے جاتے ہیں۔ گرانڈ جیوری کا پروانۂ طلبی ذاتی طور پر آپ کو ہی پیش کیا جانا چاہیے، مطلب یہ کہ آپ کے ہاتھوں میں ہی دیا جانا چاہیے۔ اگر آپ اسے قبول کرنے سے انکار کرتے ہیں تو، اسے آپ کے پاس رکھ دیا جانا چاہیے۔

گرانڈ جیوری کا پروانۂ طلبی ایجنٹ کو آپ کے گھر، دفتر، کار یا کسی اور جگہ کی تلاشی لینے کا حق نہیں دیتا ہے، نہ ہی یہ آپ سے کوئی دستاویز حوالے کرنے یا اس وقت کچھ اور بات کہنے کا تقاضہ کرتا ہے۔ گرانڈ جیوری کا پروانۂ طلبی آپ سے صرف اس بات کا متقاضی ہوتا ہے کہ پروانۂ طلبی پر مذکور آئندہ کی تاریخ میں کوئی کام کریں۔

اگر کوئی ایجنٹ آپ کو پروانۂ طلبی دکھاتا اور پیش کرنے کی کوشش کرتا ہے تو، اسے لے لیں اور اس کے علاوہ کچھ بھی نہ کریں۔ کسی سوال کا جواب نہ دیں؛ تلاشی کی منظوری نہ دیں؛ اور کسی بھی وجہ سے انہیں اپنے گھر کے اندر گھسنے کی دعوت نہ دیں۔

## گرانڈ جیوری کی پروانہ طلبی

گرانڈ جیوری پروانۂ طلبی جاری کرکے لوگوں سے معلومات حاصل کرتی ہے۔ گرانڈ جیوری کا پروانۂ طلبی گرانڈ جیوری کے سامنے گواہی دینے یا مخصوص معلومات فراہم کرنے کا فرمان ہوتا ہے۔ گرانڈ جیوری گواہی اور معلومات کے لئے مختلف قسم کا پروانۂ طلبی جاری کرتی ہے۔ subpoena ad testifi candum، یا گواہی گواہ کو حاضر ہونے اور گواہی دینے کے فرمان پر مشتمل ایک پروانۂ طلبی ہوتا ہے۔ subpoena duces tecum، جس کا مطلب لاطینی میں "اسے اپنے ساتھ لائیں" ہوتا ہے، گواہ کو گرانڈ جیوری کو مخصوص دستاویزات فراہم کرنے پر مشتمل پروانۂ طلبی ہوتا ہے۔ گرانڈ جیوری انگلیوں کے نشانات اور دستی تحریر کے نمونے حاصل کرنے کے لئے بھی یہ فرامین جاری کرتی ہے۔ گرانڈ جیوری بیشتر اوقات ایک ہی گواہ کے لئے دونوں طرح کے پروانۂ طلبی جاری کرتی ہے تاکہ وہ دستاویزات اور گواہی دونوں ہی حاصل کرسکیں۔

## ان کے وسائل کو جانیں

## اگر مجھے گرانڈ جیوری کا پروانہ طلبی موصول ہوتا ہے تو مجھے کون سے اختیارات حاصل ہیں؟

گرانڈ جیوری کا پروانۂ طلبی موصول ہوجانے پر، آپ کو خاص طور پر تین اختیارات ہوتے ہیں: 1) آپ پروانۂ طلبی کی تعمیل کرسکتے ہیں؛ 2) آپ پروانۂ طلبی کو کالعدم قرار دینے کی کارروائی کرسکتے ہیں؛ یا 3) آپ تعمیل کرنے سے انکار کرسکتے ہیں۔ اگر آپ کو پروانۂ طلبی موصول ہوتا ہے تو، جتنی جلدی ممکن ہوسکے آپ کو کسی وکیل سے رابطہ کرکے ان میں سے ہر ایک اختیار پر پوری تفصیل سے گفتگو کرنا چاہیے۔

پروانۂ طلبی کی تعمیل کرنا نسبتا سیدھا سادا ہے۔ subpoena ad testifi candum کے لئے آپ کو پروانۂ طلبی میں مذکورتاریخ ، وقت اور مقام پر پہنچنا اور استغاثہ کے سوالوں کا جواب دینا چاہیے۔ subpoena duces tecum کے لئے آپ کو پروانۂ طلبی میں مذکورتاریخ ، وقت اور مقام پر مطلوبہ دستاویزات یا دیگر ثبوت دکھانا چاہیے۔

اگر آپ پروانۂ طلبی کی تعمیل کرتے ہیں تو، گویا آپ اسے نظر انداز کرنے پر سزا دیئے جانے کے امکان سے احتراز کرتے ہیں؛ تاہم، پروانۂ طلبی کی تعمیل سے مختلف قسم کی پریشانی لاحق ہونے کا امکان ہے۔ مثال کے طور پر، اگر آپ کو چھان بین کا ہدف بنایا گیا ہے تو، پروانۂ طلبی کی تعمیل سے حکومت کو ایسی معلومات فراہم ہوسکتی ہے جو اسے آپ پرالزام عائد کرنے اور ملزم قرار دینے کے لئے درکار ہوسکتی ہے۔ آپ پروانۂ طلبی کی تعمیل کرکے دیگر فعالیت پسند کو بھی خطرے میں ڈال سکتے ہیں۔

اگر آپ کو پروانۂ طلبی موصول ہوتا ہے تو، کوئی بھی کارروائی کرنے سے پہلے آپ کو وکیل سے بات کرنی چاہیے۔ اگر پروانۂ طلبی کو سیاسی لحاظ سے تحریک ملی ہے تو، آپ کو اپنی دائرہ سرگرمی میں ایسے وکیل سے بات کرنی چاہیے جو مجرمانہ مدافعت یا گرانڈ جیوری کا کام کرتا ہے۔ کچھ

## اگر مجھے گرانڈ جیوری کا پروانہ طلبی موصول ہوتا ہے تو مجھے کون سے اختیارات حاصل ہیں؟ (جاری...)

غیر فعالیت پسند مجرمانہ مدافعت والے وکیل آپ کو مخبر بن جانے کی صلاح دے سکتے ہیں۔ تاہم، یہ یاد رکھنا ضروری ہے کہ بہت سارے مخبرانہی افراد کی طرح سالوں تک جیل میں زندگی گزار دیتے ہیں جن کی انہوں نے مخبری کی ہوتی ہے۔

گرانڈ جیوری کی کارروائیاں مخفی ہوتی ہیں۔ فعالیت پسند برادری کو اکثر معلوم نہیں ہوتا ہے کہ گرانڈ جیوری کی چھان بین کا عمل کب انجام پاتا ہے۔ نتیجے کے طور پر، بہت سارے فعالیت پسند یہ مانتے ہیں کہ وہ اس حقیقت کی تشہیر کریں گے کہ انہیں پروانۂ طلبی موصول ہوا ہے۔ اگر آپ کو پروانۂ طلبی موصول ہوا ہے تو، یہ آپ کے وکیل سے پتہ کرنے کا ایک مؤثرحربہ ہوسکتا ہے۔

## میں گرانڈ جیوری کے پروانہ طلبی کو کس طرح کالعدم قرار دوں؟

آپ پروانۂ طلبی کو کالعدم قرار دینے کے تحریک پش کرکے عدالت میں اس پروانۂ طلبی کو چیلنج کرسکتے ہیں۔ پروانۂ طلبی کو کالعدم قرار دینے کا مطلب یہ ہوتا ہے کہ عدالت اسے باطل یا لایعنی قرار دیتی ہے۔ عدالت باطل قرار دینے کی تحریک صرف اسی صورت میں منظور کرے گی جب معقول قانونی بنیاد موجود ہو، جیسے غلط نشاندہی؛ دائرہ اختیار کا فقدان؛ تحفظ یافتہ رعایت؛ یا کارروائیاں کرنے کے لئے غیر قانونی بنیاد۔

یہاں تک کہ اگر آپ کامیابی کے ساتھ پروانۂ طلبی کو کالعدم قرار نہیں دے سکتے ہیں تو، عدالت میں اسے کالعدم قرار دینے کی چارہ جوئی میں تھوڑا وقت لگ سکتا ہے۔ وقت اہم ہے ، خاص طور پر اگر آپ کا ارادہ گرانڈ جیوری کے ساتھ تعاون کرنے کا نہیں ہے، کیونکہ عدم تعاون کی وجہ سے آپ کو جیل جانا پڑسکتا ہے۔ گرانڈ جیوری کی کارروائی 18 مہینوں تک چل سکتی ہے؛ کالعدم قرار دینے کی چارہ جوئی میں چاہے جتنا بھی وقت صرف ہو اس سے آپ کا یہ پورا عرصہ جیل میں گزرنے سے بچ سکتا ہے۔

یوں تو subpoena duces tecum کالعدم قرار دینے کی عرضی سے محرومی کا تھوڑا سا امکان ہے، مگر ثبوت کے طالب پروانۂ طلبی، subpoena duces tecum کالعدم قرار دینے کی تحریکیں، جو گواہی کی طالب ہوتی ہیں، پریشانیاں کھڑی کرسکتی ہیں۔ کم از کم ایک وفاقی سرکٹ عدالت نے یہ فرمان صادر کیا کہ آپ کسی بھی ایسے اعتراض سے محروم ہوجائیں گے جو کالعدم قرار دینے کی اصل تحریک میں نہیں اٹھایا گیا تھا۔ آپ کو خاص طور پر یہ معلوم نہ ہونے کی وجہ سے کہ آپ سے کوئی مخصوص سوال پوچھے جانے پر آپ کو کیا اعتراضات ہیں، اپنے اعتراضات سے دستکش نہیں ہونا چاہیے ۔

ایک اچھا سیاسی وکیل آپ کو اس ضمن میں معلومات فراہم کرنے کا اہل ہونا چاہیے کہ آیا آپ کے مخصوص حالات میں اسے خارج قرار دینے کی تحریک پیش کرنا ایک اچھا خیال ہے یا نہیں۔

## اگر میں گرانڈ جیوری کے پروانہ طلبی کی تعمیل سے انکار کرتا ہوں تو کیا ہوتا ہے؟

گرانڈ جیوری کے پروانۂ طلبی کی تعمیل سے انکار کرنے کے دو بنیادی طریقے ہیں: 1) حاضر ہونے سے انکار کریں؛ اور 2) استغاثہ کے کسی بھی وکیل کا جواب دینے سے منع کردیں۔

اگر آپ سیدھے سیدھے اپنی گواہی کے لئے حاضر ہونے سے انکار کرتے ہیں تو، آپ حکم عدولی کے مرتکب ہوسکتے ہیں اور عدالت آپ کو گرفتار کرکے جیل میں ڈالنے کا انتخاب کرسکتی ہے تاوقتیکہ آپ گواہی دے دیں یا گرانڈ جیوری کی مدت ختم ہوجائے۔ اگر آپ کی گواہی استغاثہ کے لئے خصوصی اہمیت کی حامل نہیں ہے تو، وہ کوئی کارروائی نہ کرنے کا بھی انتخاب کرسکتے ہیں۔

## اگر میں گرانڈ جیوری کے پروانہ طلبی کی تعمیل کرتا ہوں تو کیا ہوتا ہے؟

اگر آپ گواہی کے لئے حاضر ہوتے ہیں تو، آپ کو وکیل موجود رکھنے کی اجازت نہیں ہوگی۔ تاہم، آپ گرانڈ جیوری کے کمرے سے خارج میں ایک وکیل رکھ سکتے ہیں، اور ہر سوال کے بعد ان سے رجوع کرسکتے ہیں۔ چونکہ خود کو مجرم قرار دیئے جانے کے خلاف آپ کو اپنی پانچویں ترمیم کا حق حاصل ہے، لہذا آپ ہر سوال کے بعد یہ کہہ کر استغاثہ کے سوالوں کا جواب دینے سے انکار کرسکتے ہیں کہ "میں خود کو ملزم قرار دینے کے خلاف اپنی پانچویں ترمیم کی رعایت کو کالعدم قرار دیتا ہوں۔ اس موقع پر، استغاثہ بس آپ کو معطل قرار دے سکتا ہے یا وہ آپ کی مامونیت کی منظوری حاصل کرسکتا ہے۔

مامونیت گرانڈ جیوری کی گواہی کی بنیاد پر گواہ کے اوپر مجرمانہ دفعات عائد کرنے کو ممنوع قرار دیتی ہے۔ جج کو چاہیے کہ مامونیت کو منظوری دے۔ استغاثہ جج سے مامونیت کو منظوری دلوا سکتا ہے؛ بصورت دیگر، گواہ کو جج کے سامنے پیش کیا جاسکتا ہے، جو استغاثہ کی درخواست پر، اخلاقی طور پر ہمیشہ ہی مامونیت کو منظوری دیتا ہے۔

اگر آپ مامونیت منظور ہوجانے کے بعد سوالوں کا جوب دینے سے انکار کرتے رہتے ہیں تو، استغاثہ آپ کو جج کے سامنے پیش کرسکتا ہے، اور جج آپ کو گواہی دینے کا حکم دے گا۔ اگر آپ انکار کرتے رہتے ہیں تو، جج آپ کو دیوانی حکم عدولی کے الزام میں جیل میں ڈال سکتا ہے۔ ایسے گواہان جو گرانڈ جیوری کی درخواست پر طبعی موجودگی، جیسے دستی تحریر کے نمونے، بال، قطار بندی میں حاضری یا دستاویزات فراہم کرنے سے انکار کرتے ہیں انہیں بھی دیوانی حکم عدولی کے الزام میں جیل میں ڈالا جاسکتا ہے۔

یوں تو دیوانی حکم عدولی کوئی جرم نہیں ہے، مگر اس کے نتیجے میں گواہ کو گرانڈ جیوری کی مدت تک کے لئے جیل میں ڈالا جاسکتا ہے۔ گرانڈ جیوری 18 ماہ کے عرصے تک قائم رہ سکتی ہے، حالانکہ کچھ "مخصوص" گرانڈ جیوری چھ چھ ماہ کے عرصے کی توسیع تین بار تک حاصل کرسکتی ہیں۔ کسی منحرف گواہ کو زیر حراست کرکے رکھنے کا مقصد انہیں گواہی دینے پر مجبور کرنا ہوتا ہے۔ اگر یہ واضح ہوجائے کہ گواہ کو گواہی دینے کا کوئی امکان نہیں ہے تو جج صاحبان کبھی کبھی جیوری کی مدت ختم ہونے سے پہلے گواہوں کو رہا کرسکتے ہیں۔

## اگر میں گرانڈ جیوری کے پروانہ طلبی کی تعمیل کرتا ہوں تو کیا ہوتا ہے؟ (جاری...)

حکومت "فوجداری حکم عدولی" کے الزام کو گرانڈ جیوری کے ساتھ اعانت نہ کرنے والے گواہوں کے خلاف بھی استعمال کرسکتی ہے۔ فوجداری حکم عدولی میں زیادہ سے زیادہ جرمانہ نہیں ہوتا ہے - سزا یابی کا انحصار کلی طور پر جج کی صوابدید پر منحصر ہوتا ہے۔ یوں تو دیوانی حکم عدولی کا مقصد گواہ کو گواہی دینے پر مجبور کرنا ہوتا ہے، مگر فوجداری حکم عدولی قانونی کارروائیوں کو التواء میں ڈالنے کی وجہ سے گواہ کو سزا دینے کے لئے ہوتی ہے۔ جیسا کہ دیگر کسی بھی جرم کے معاملے میں ہوتا ہے، فوجداری حکم عدولی الزامات کی اطلاع، مشیر کی اعانت حاصل کرنے کے حق، اور معقول شبہے سے ماوراء ثبوت کی متقاضی ہوتی ہے۔ فوجداری حکم عدولی کے الزامات بہت ہی شاذ و نادر ہوتے ہیں۔

اگر آپ کو جیل میں ڈال دیا گیا ہے تو، آپ وقفے وقفے سے یہ بیان کرتے ہوئے ایک تحریک پیش کرسکتے ہیں کہ: 1) جیل آپ کو گواہی دینے پر مجبور نہیں کرپائے گی؛ اور 2) آپ کو زیر حراست رکھنا محض سزا دینے کے لئے ہے اور اسی وجہ سے یہ غیر آئینی ہے۔ اگر آپ ان میں سے کوئی بھی تحریک جیت لیتے ہیں تو، آپ کو رہا کردیا جائے گا۔

کچھ فعالیت پسند گرانڈ جیوری کے سامنے طلب جانے کے واسطے تیاری کرنے کے لئے فائلیں بناتے ہیں۔ گرانڈ جیوری کی کارروائیوں میں تعاون کرنے کے برخلاف آپ کی ٹھوس رائے پر مشتمل ایک یاد داشت ایک ثبوتکے طور پر استعمال ہوسکتی ہے کہ دیوانی حکم عدولی آپ کو جھکنے پر مجبور نہیں کرے گی اور اس طرح آپ کی رہائی میں معاون ہوسکتی ہے۔

## گرانڈ جیوری کے بعد کیا ہوتا ہے؟

گرانڈ جیوری کی کارروائیوں میں جو بھی معاملہ پیش آتا ہے وہ راز میں رہتا ہے۔ حکومت کسی فعالیت پسند برادری میں خوف اور بے اعتمادی پیدا کرنے کے لئے ان خفیہ امور پر بھروسہ کرتی ہے۔ کچھ فعالیت پسندوں نے استغاثہ کی جانب سے خود سے پوچھے جانے والے سوالات اور ان کے فراہم کردہ جوابات کی تشہیر کرکے فعالیت پسند برادریوں میں اس خوف اور بے اعتمادی کا خاتمہ کامیابی کے ساتھ کیا ہے۔ اگر آپ اس طرح سے کارروائی کرنے پر غور کر رہے ہیں تو، آپ کو یہ یقینی بنانے کے لئے وکیل سے لازما بات کرنی چاہیے کہ آپ جتنے مسائل حل کر رہے ہیں اس سے زیادہ مسائل پیدا تو نہیں کر رہے ہیں۔

# غیرملکیوں کے لئے
# خصوصی طورپرزیرغورامور

غیر ملکی وہ افراد ہوتے ہیں جن کے پاس امریکی شہریت نہیں ہے، بشمول سیاح، طلباء اور دیگر ایسے افراد جو ویزا پر یا ویزا سے تخفیف کے پروگراموں کی بناء پر امریکہ میں ہیں؛ قانونی طور پر مستقل شہری؛ پناہ گزین؛ اور ایسے افراد جن کی ترک وطنی کی قانونی حیثیت نہیں ہے۔ امریکہ میں رہنے والے غیر ملکی یہاں کے شہریوں کی طرح ہی بیشتر دستوری حقوق کا اشتراک کرتے ہیں۔ اس اصول میں کچھ استثناء بھی ہے، اور سیاسی سرگرمی میں مصروف غیر ملکیوں کو متعدد خصوصی زیر غور امور سے واقف رہنا چاہیے۔ تاہم، غیر ملکیوں کو حکومت کے دباؤ کے کسی نامناسب خوف کی بناء پر سیاسی سرگرمی سے کلی طور پر احتراز بھی نہیں کرنا چاہیے۔

## تقریراورسیاسی وابستگیاں

زیادہ تر معاملات میں، حکومت غیر ملکیوں کی تقریروں کو شہریوں کے ذریعہ کی جانے والی تقریروں جیسی ہی مانتی ہے۔ غیر ملکیوں کو ایسی تقریر کے لئے تعزیری سزائیں نہیں دی جاسکتی ہیں کہ اگر یہ تقریر کسی شہری کے ذریعہ کی گئی ہوتی تو اسے تحفظ فراہم کیا جاتا۔ اسی طرح، غیر ملکی کو ایسی تقریر کے لئے کارروائی کا مستوجب قرار نہیں دیا جاسکتا ہے کہ اگر یہ تقریر کسی شہری کے ذریعہ کی گئی ہوتی تو تحفظ یافتہ ہوتی۔ تاہم حکومت کے پاس ترک وطنی کی مراعات کو معطل کرنے کے لئے وسیع پیمانے کے اختیارات ہیں (جیسے صوابدیدی راحت یا حصول شہریت) اور یہاں تک کہ امکانی طور پر غیر ملکی کی تقریر کی بنیاد پر اسے دیس نکالا دینے کی کارروائی بھی شروع کرسکتی ہے۔ یہ امر واضح نہیں ہے کہ آیا حکومت محض تقریر یا سیاسی وابستگی کے چلتے غیر ملکی کو دیس نکالا دے سکتی ہے یا صوابدیدی مراعات معطل کرسکتی ہے۔ پچاس سال پہلے، کچھ عدالتیں اس نتیجے پر پہنچیں کہ حکومت ایسا کرسکتی ہے، لیکن پہلی ترمیم کے قانون سے اس کے بعد ڈرامائی طور پر تبدیلی آئی ہے، اور کچھ عدالتیں اب اس بابت مختلف الرائے ہیں کہ آیا یہ اصول ابھی بھی ایک اچھا قانون ہے۔ عملی لحاظ سے بات کریں تو، شاذ و نادر ہی ایسا ہوتا ہے کہ حکومت صرف اور صرف تقریر یا وابستگی کی بناء پر کسی کو دیس نکالا دیتی ہے۔ تاہم، حکومت کو چننده طور پر ترک وطنی کے قوانین کو بروئے کار لانے کی اجازت ہے۔ مثال کے طور پر، حکومت ترک وطنی کے قانون کی خلاف ورزی پر (مثلاً، ویزا سے زیادہ مدت تک قیام کرنے، یا اجازت کے بغیر کام کرنے پر) غیر ملکیوں کو دیس نکالا دے سکتی ہے چاہے دیس نکالا دینے کی کارروائی شروع کرنے سے حکومت کا مقصد کسی غیر ملکی کی تقریر یا سیاسی وابستگی ہی ہو۔

## تقریر اور سیاسی وابستگیاں (جاری...)

آخری بات، مستقل اقامت اور حصول شہریت کے درخواست دہندگان سے ایسی تنظیموں کی فہرست تیار کرنے کا تقاضہ کیا جاتا ہے جن کے لئے انہوں نے کام کیا ہوتا ہے۔ سیاسی طور پر فعال غیر ملکیوں کو اس حیثیت میں بدلاؤ کے لئے درخواست دینے سے پہلے ترک وطنی سے متعلق وکیل سے رابطہ کرنے کا مشورہ دیا جاتا ہے کیونکہ کچھ انجمنیں آپ کی درخواست دہندگی کی کارروائی میں دشواریاں پیدا کرسکتی ہیں۔

## تلاشیاں اور ضبطیاں

غیر ملکی وسیع پیمانے پر غیر مناسب تلاشیوں اور ضبطیوں کے خلاف چوتھی ترمیم کی انہی تحفظات کا فائدہ اٹھا سکتے ہیں جن کا فائدہ شہری اٹھا سکتے ہیں۔ نفاذ قانون سے متعلق اہلکار کو کسی غیر ملکی کی یا غیر ملکی کے املاک کی تلاشی لینے کے لئے اسی طرح سے وارنٹ حاصل کرنا چاہیے جس طرح شہریوں کی تلاشی لینے کے لئے حاصل کرنا ہوتا ہے۔ چوتھی ترمیم کے برخلاف حاصل کردہ ثبوت غیر ملکیوں کی فوجداری سماعت میں اسی طرح سے خارج ہوتی ہے جس طرح وہ شہریوں کے لئے ہے۔
بدقسمتی سے، چوتھی ترمیم کے برخلا حاصل کردہ ثبوت کو عام طور پر ترک وطنی کی قانونی کارروائیوں میں استعمال کرنے کی اجازت ہوتی ہے۔ اس کا مطلب یہ ہوتا ہے کہ حکومت غیر قانونی طریقے سے حاصل کردہ ایسی معلومات استعمال کرسکتی ہے جسے ترک وطنی کی کارروائیوں کے لئے فوجداری کارروائیوں میں استعمال نہیں کیا جاسکتا ہے۔ اس امر کا امکان ہے کہ خاص طور پر چوتھی ترمیم کی سنگین خلاف ورزیوں سے حاصل شدہ معلومات کو ترک وطنی کی کارروائیوں میں خارج کردیا جائے۔

نیز، حکومت عام طور پر سرحد کے قریب یا ہوائی اڈے کے پاس سے گزرنے والے کسی بھی فرد، پیکیج یا گاڑی کی تلاشی لے سکتی اور اسے ضبط کرسکتی ہے۔

## چپ رہنے کا حق

غیر ملکیوں کو بھی عام طور پر چپ رہنے کا ویسا ہی حق حاصل ہے جس طرح شہریوں کو حاصل ہے۔ اگر نفاذ قانون سے متعلق اہلکار کے ذریعہ پوچھ تاچھ کی جاتی ہے تو، آپ بدستور خاموش رہ سکتے اور ان کے سوالوں کا جواب دینے سے انکار کرسکتے ہیں خواہ وہ عارضی طور پر آپ کو زیر حراست رکھیں یا گرفتار کرلیں۔ آپ یا تو ان سے کچھ نہیں کہیں گے یا آپ صرف یہ کہہ سکتے ہیں کہ "میں آپ سے کچھ بھی کہنے سے پہلے اپنے وکیل سے بات کرنا چاہوں گا"یا "مجھے آپ سے کچھ نہیں کہنا ہے۔ میں اپنے وکیل سے بات کروں گا اور ان کو آپ سے رابطہ کرنے کو کہوں گا۔" کسی بھی چیز پر دستخط نہ کریں جب تک آپ اسے پڑھ نہ لیں اور اس پر دستخط کرنے کے عواقب کو سمجھ نہ لیں۔
اس اصول میں ایک استثناء اس صورت میں ہے جب ترک وطنی سے متعلق افسر غیر ملکی سے اپنی ترک وطنی سے متعلق معلومات فراہم کرنے کو کہتا ہے؛ تاہم، اس صورتحال میں بھی، آپ یہ کہہ سکتے ہیں کہ آپ کسی بھی سوال کا جواب دینے سے پہلے وکیل کو پیش کرنا چاہیں گے۔

## چپ رہنے کا حق (جاری...)

قانون اس امر کا بھی متقاضی ہے کہ موزوں قانونی دستاویزات کے حامل بالغ غیر ملکی شہری یہ دستاویزات ہمہ وقت اپنے ساتھ رکھیں۔ اگر کوئی ایجنٹ آپ کے دستاویزات طلب کرتا ہے اور آپ انہیں فراہم کرنے سے انکار کرتے ہیں تو، آپ پر خفیف جرم کا الزام عائد ہوسکتا ہے۔
یہ دعوی کرنے کے لئے کہ آپ امریکی شہر ی ہیں یا آپ امریکی شہری نہیں ہیں کبھی بھی ترک وطنی کے جعلی کاغذات نہ دکھائیں۔ اس کے بجائے، آپ کو چپ رہنا چاہیے یا یہ کہنا چاہیے کہ آپ اپنے وکیل سے بات کریں گے۔ وفاقی افسر کے سامنے جھوٹ بولنا خفیف جرم یا دستاویزات پیش نہ کرپانے کی بہ نسبت زیادہ سنگین جرم ہے – جعلی کاغذات پیش کرنے سے بہتر ہے کہ کچھ بھی نہ پیش کیا جائے۔ نیز، شہری بننے کے لئے جعلی طور پر دعوی دائر کرنا آپ کو آئندہ قانونی حیثیت یا شہریت حاصل کرنے میں مانع بن سکتا ہے۔

# اختتامیہ

جیسا کہ اوپر بیان کیا گیا، اس کتابچہ میں پیش کردہ معلومات آپ کے بنیادی حقوق کے سلسلے میں ایک پیشرو ہے۔ یہ رہنما کتابچہ کسی ایجنٹ کے آپ کے دروازے پر دستک دینے کی صورت میں اپنی ذات، اپنی تنظیم اور اپنے ساتھی فعالیت پسندوں کو پوری طرح سے باخبر رکھنے اور تحفظ فراہم کرنے میں آپ کی مدد کرنے کے ارادے سے بنایا گیا ہے۔ اور یاد رکھیں، مختلف ریاستوں میں مختلف قوانین ہیں – اپنی ریاست کے قوانین کو جان لینا اور ان قوانین کی واقفیت رکھنے والے کسی وکیل تک رسائی حاصل کرنا اچھا خیال کیا جاتا ہے۔
ہمیں امید ہے کہ یہ کتابچہ آپ اور آپ کی تنظیم کے لئے ایک وسیلہ ثابت ہوسکتا ہے کیونکہ ہم سماجی لحاظ سے ایک زیادہ انصاف پسند دنیا کے تئیں کام کرتے ہیں۔
اس اشاعت کی نقول کے لئے براہ کرم http://ccrjustice.org/ifanagentknocks ملاحظہ کریں یا iaak@ccrjustice.org پر براہ راست خط لکھیں۔

# اضافی وسائل

## عمومی سلامتی کے طرز عمل کے بارے میں:

**تحفظاتی ثقافت**: فعالیت پسندوں کے لئے ایک دستی کتابچہ کینیڈین فعالیت پسندوں کے ذریعہ ایک عمدہ رسالہ اس ضمن میں کہ تحفظاتی ثقافت کی تشکیل کیسے کی جائے اور اس پر کیسے کاربند رہا جائے۔
http://security.resist.ca/personal/culture.shtml

**سیکیورٹی کی تفحظاتی اھلیتیں، پولیس کی بربریت کے برخلاف اجتماعیت کے لحاظ سے**: اس ضمن میں ایک وضاحت کہ کینیڈا کے گروپوں سے تعلق رکھنے والی آپ کی فعالیت پسند برادری میں تحفظاتی ثقافت کی تشکیل کیسے کی جائے۔
http://www.why-war.com/fi les/Securite-eng-letter.pdf

**گھریلو جنگ، از برائن گلک**: COINTELPRO کی تاریخ پر ایک جامع کتاب اور اس ضمن میں عمدہ مشورہ کہ ایک جیسی غلطی سے کیسے بچا جائے اور اپنی ذات کو اور اپنے معاشرے کو کیسے تحفظ فراہم کیا جائے۔ شائع کردہ ساؤتھ اینڈ پریس۔

## حکومت کے ایجنٹوں کے بارے میں:

**FBI کے خفیہ اعمال کے تعلق سے اٹارنی جنرل کی رھنما خطوط**: اس ضمن میں وفاقی حکومت کے اصول کے خفیہ ایجنٹ کیا کام کرسکتے ہیں اور کیا کام نہیں کرسکتے ہیں۔
http://www.usdoj.gov/olp/fbiundercover.pdf

**خفیہ مخبروں کے استعمال کے سلسلے میں اٹارنی جنرل کی رھنما خطوط**: اس ضمن میں وفاقی حکومت کے اصول کے مخبر کیا کام کرسکتے ہیں اور کیا کام نہیں کرسکتے ہیں۔
http://www.usdoj.gov/olp/dojguidelines.pdf

**تحفظاتی طرز عمل اور تحفظاتی ثقافت**: COINTELPRO عہد سے خفیہ اعمال سے اور عظیم وقوعات سے نمٹنے کے لئے بنیادی نکات۔
http://aia.mahost.org/sec_cointelpro.htm

## ٹیلیفون سیکیورٹی کے بارے میں:

**موبائل سرویلنس پرائمر**: سیل فون کی ٹکنالوجیز، ان تک رسائی کے طریقے، اور ان میں ذخیرہ کردہ معلومات اور آپ کی گفتگو کو تحفظ فراہم کرنے کے طریقے سے متعلق ایک مکمل آن لائن وسیلہ http://mobileactive.org/wiki/Mobile_Surveillance-A_Primer

## نیشنل سیکیورٹی لیٹرز کے بارے میں:

**نیشنل سیکیورٹی لیٹرز کے FBI کے استعمال کا ایک جائزہ، از ڈپارٹمنٹ آف جسٹس:** نیشنل سیکیورٹی لیٹرز کے قانون اور ان کی تشریح کے بعد سے جس طریقے سے ان کا استعمال ہوا ہے ان کا ایک مکمل تجزیہ۔
http://www.usdoj.gov/oig/special/s0703b/fi nal.pdf

## کمپیوٹر سیکیورٹی کے بارے میں:

**کمپیوٹر سیکیورٹی کے ترتیب دھندہ کا رھنما کتابچہ، از مڈنائٹ اسپیشل لاء کلیکٹو:** سافٹ ویئر یا تکنیکی چالبازیوں کے بجائے کمپیوٹر کے معاملے میں تحفظ کی اچھی عادات کو فروغ دینے سے متعلق ایک واقعتا عمدہ رہنما کتابچہ۔
http://www.midnightspecial.net/materials/trainers.html

**NGO ان اے باکس: سیکیورٹی ایڈیشن، از ٹکٹیکل ٹکنالوجی کلیکٹو اور فرنٹ لائن ھیومن رائٹس ڈیفینڈرز:** ڈیجیٹل سیکیورٹی تشکیل دینے اور ان کی رازداری کو تحفظ فراہم کرنے کے واسطے فعالیت پسندوں اور خود مختار ذرائع ابلاغ سازوں کی مدد کے لئے ایک ٹول کٹ۔ اس ٹول کٹ میں مرموز کاری والے ٹولز؛ وائرس، ایڈ ویئر اور اسپائی ویئر کلینر ٹولز؛ ڈیٹا کی ذخیرہ اندوزی؛ پاسورڈ کا تحفظ؛ وغیرہ کے ضمن میں رہنما ہدایات شامل ہیں۔ انٹرنیٹ پر مفت میں دستیاب ہے۔
http://security.ngoinabox.org

**سرویلنس سیلف ڈیفنس، از الیکٹرانک فرنٹیئر فاؤنڈیشن:** اس ضمن میں ایک عمدہ آن لائن وسیلہ کہ ہر قسم کی الیکٹرانک نگرانی سے خود کو کیسے محفوظ رکھا جائے۔ کمپیوٹر سیکیورٹی کی خصوصی معلومات کے لئے، "آپ کے کمپیوٹر پر ذخیرہ کردہ ڈیٹا" اور "دفاعی ٹکنالوجی" ملاحظہ کریں۔
https://ssd.eff.org

## ھائی ٹیک نگرانی کے بارے میں:

**بڑے گھڑیال، کمزور زنجیریں: امریکی نگرانی والے ایک معاشرے کا ارتقاء، از ACLU:** نگرانی والے کیمروں اور دیگر ٹکنالوجیوں کی حالیہ تاریخ کے بارے میں ایک قرطاس ابیض ۔
http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf

## گرانڈ جیوری کے بارے میں:

**گرانڈ جیوری کے تربیت دھندگان کا رھنما، از مڈنائٹ اسپیشل لاء کلیکٹو:** گرانڈ جیوریز کی ایک وضاحت – وفاقی ایجنٹوں کے ساتھ پہلے رابطے سے لے کر بذات خود گرانڈ جیوری کی سماعت تک – اور اگر آپ کو کسی کے سامنے حاضر ہونے کو کہا جاتا ہے تو خود کو اور اپنے معاشرے کو تحفظ فراہم کرنے کا طریقہ۔
http://www.midnightspecial.net/materials/trainers.html#gj

**اعلان دستبرداری :** یہ کتابچہ صرف معلوماتی مقاصد کے لئے ہے اور یہ کسی قانونی مشورے کو مستلزم نہیں ہے۔ CCR کا مقصد ایسے قانونی اور عملی امور کی ایک عمومی وضاحت فراہم کرنا ہے جن کا سامنا ترقی پسند یا انتہا پسند فعالیت پسندوں کو ہوسکتا ہے۔ ہر فرد کے حالات منفرد ہوتے ہیں، اور حقائق میں معمولی سے فرق کے نتیجے میں یہاں پیش کردہ سوالوں کے جوابات میں کافی فرق آسکتا ہے۔ مخصوص قانونی دشواریوں، مسائل یا سوالات کے جوابات کے لئے، اپنے علاقے کے کسی مستند وکیل سے مشورہ حاصل کریں۔

## اعترافات اور انتسابات

**سنٹر فار کانسٹی ٹیوشنل رائٹس (مرکز برائے دستوری حقوق)**
**Broadway, 7th Floor 666**
**New York, NY 10012**
**www.CCRJustice.org / (212) 614-6464**

سنٹر فار کانسٹی ٹیوشنل رائٹس (CCR) ریاستہائے متحدہ کے دستور اور انسانی حقوق کے عالمی اعلامیہ کے ذریعہ ضمانت یافتہ حقوق کو آگے بڑھانے اور تحفظ فراہم کرنے کے لئے وقف ہے۔ ساؤتھ میں دیوانی حقوق کی تحریکوں کی نمائندگی کرنے والے وکلاء کے ذریعہ 1966 میں قائم کردہ، CCR ایک غیر منفعتی قانونی اور تعلیمی تنظیم ہے اور سماجی بدلاؤ کے لئے ایک مثبت طاقت کے بطور قانون کے تخلیقی استعمال کے تئیں عہد بستہ ہے۔ ملاحظہ کریں www.ccrjustice.org

اصل مصنف، میتھیو اسٹریوجر Matthew Strugar ، CCR اسٹاف اٹارنی۔
"اگر کوئی ایجنٹ دستک دیتا ہے" CCR کے عملہ اور زیر حراست افراد، بشمول لاؤرین میلوڈیا (Lauren Melodia)، رشیل میروپول (Rachel Meeropol)، الیسن رو پارک (Alison Roh Park)، قائد جیکبس (Qa'id Jacobs)، جیف ڈیوش (Jeff Deutch)، عروہ فدا حسین (Arwa Fidahusein)، کیتھ جیفونی (Cathe Giffuni)، ٹونی ہالنیس (Toni Holness)، کیرولن سو (Carolyn Hsu)، جیسیکا جوریز (Jessica Juarez)، کینیتھ کریور (Kenneth Kreuscher)، ڈیوڈ منڈیل (David Mandel) - اٹارنی اور کرسٹینا اسٹیفنسن Christina Stephenson) کے ذریعہ تیار کیا گیا تھا۔

ترجمہ اردو میں اصل متن: Morningside Translations
سر ورق کی فنکانی رابرٹ ٹریوجیلو (2009) (Robert Trujillo)
تصویر کشی بذریعہ میڈی ملّر (Maddy Miller) (صفحہ 5,9,15)
تصویر کشی بذریعہ SSGT رینالو ریمن (SSGT Reynoldo Ramon), USAF)صفحہ 21)
تصویر کشی بذریعہ جیرک ٹیوزنسکی (Jarek Tuszynski) (صفحہ 36)
استعمال شدہ فونٹس: Georgia (body), Distro (headers), Fluoxetine (headers)
تصویری علامات بذریعہ pixel-mixer.com
خاکہ: قائد جیکبس، أحمد فوله

centerforconstitutionalrights

*on the front lines for social justice*